Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
Application					
Ncomputing					
Vspace Pro					
Directory Traversal	20-04-2018	5	An issue was discovered in NcMonitorServer.exe in NC Monitor Server in NComputing vSpace Pro 10 and 11. It is possible to read arbitrary files outside the root directory of the web server. This vulnerability could be exploited remotely by a crafted URL without credentials, with .../ or ... or ..../ or.... as a directory-traversal pattern to TCP port 8667. **CVE-ID:CVE-2018-10201**	https://www.kwell.net/kwell/index.php?option=com_newsfeeds&view=newsfeed&id=15&Itemid=173&lang=es, https://www.exploit-db.com/exploits/44497/	A-Nco-Vspac/16-05-18/1
Oracle					
Database Server					
NA	18-04-2018	6	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2 and 12.2.0.1. Difficult to exploit vulnerability allows low privileged attacker having Create Session, Create Procedure privilege with network access via multiple protocols to compromise Java VM. While the vulnerability is in Java VM, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java VM. CVSS 3.0 Base Score 8.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector:	NA	A-Ora-Datab/16-05-18/2

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			(CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H). **CVE-ID:CVE-2018-2841**		
Data Visualization Desktop					
NA	18-04-2018	4.4	Vulnerability in the Oracle Data Visualization Desktop component of Oracle Fusion Middleware (subcomponent: Security). The supported version that is affected is 12.2.4.1.1. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Data Visualization Desktop executes to compromise Oracle Data Visualization Desktop. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Data Visualization Desktop, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Data Visualization Desktop accessible data as well as unauthorized read access to a subset of Oracle Data Visualization Desktop accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Data Visualization Desktop. Note: Please refer to Doc ID <a "http://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=2384640.1">My	NA	A-Ora-Data/16-05-18/3

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			Oracle Support Note 2384640.1 for instructions on how to address this issue. CVSS 3.0 Base Score 8.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:C/C:L/I:H/A:H). **CVE-ID:CVE-2018-2834**		
E-business Suite					
NA	18-04-2018	5.8	Vulnerability in the Oracle Application Object Library component of Oracle E-Business Suite (subcomponent: DB Privileges). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Application Object Library. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Application Object Library accessible data as well as unauthorized access to critical data or complete access to all Oracle Application Object Library accessible data. CVSS 3.0 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N). **CVE-ID:CVE-2018-2804**	NA	A-Ora-E-bus/16-05-18/4

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
Gain Information	18-04-2018	5	Vulnerability in the Oracle Application Object Library component of Oracle E-Business Suite (subcomponent: Diagnostics). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Application Object Library. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Application Object Library accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE-ID:CVE-2018-2864**	NA	A-Ora-E-bus/16-05-18/5
Financial Services Basel Regulatory Capital Basic					
NA	18-04-2018	5.5	Vulnerability in the Oracle Financial Services Basel Regulatory Capital Basic component of Oracle Financial Services Applications (subcomponent: Portfolio, Attribution). The supported version that is affected is 8.0.x. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Basel Regulatory Capital Basic. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access	NA	A-Ora-Finan/16-05-18/6

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			to critical data or all Oracle Financial Services Basel Regulatory Capital Basic accessible data as well as unauthorized access to critical data or complete access to all Oracle Financial Services Basel Regulatory Capital Basic accessible data. CVSS 3.0 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). **CVE-ID:CVE-2018-2855**		
NA	18-04-2018	5.8	Vulnerability in the Oracle Financial Services Basel Regulatory Capital Basic component of Oracle Financial Services Applications (subcomponent: Portfolio, Attribution). The supported version that is affected is 8.0.x. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Financial Services Basel Regulatory Capital Basic. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Financial Services Basel Regulatory Capital Basic, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Financial Services Basel Regulatory Capital Basic accessible data as well as	NA	A-Ora-Finan/16-05-18/7

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			unauthorized read access to a subset of Oracle Financial Services Basel Regulatory Capital Basic accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-2854**		
Financial Services Basel Regulatory Capital Internal Ratings Based Approach					
NA	18-04-2018	5.5	Vulnerability in the Oracle Financial Services Basel Regulatory Capital Internal Ratings Based Approach component of Oracle Financial Services Applications (subcomponent: Portfolio, Attribution). The supported version that is affected is 8.0.x. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Basel Regulatory Capital Internal Ratings Based Approach. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Financial Services Basel Regulatory Capital Internal Ratings Based Approach accessible data as well as unauthorized access to critical data or complete access to all Oracle Financial Services Basel Regulatory Capital Internal Ratings Based Approach accessible data. CVSS 3.0 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS	NA	A-Ora-Finan/16-05-18/8

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). **CVE-ID:CVE-2018-2856**		
NA	18-04-2018	5.8	Vulnerability in the Oracle Financial Services Basel Regulatory Capital Internal Ratings Based Approach component of Oracle Financial Services Applications (subcomponent: Portfolio, Attribution). The supported version that is affected is 8.0.x. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Financial Services Basel Regulatory Capital Internal Ratings Based Approach. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Financial Services Basel Regulatory Capital Internal Ratings Based Approach, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Financial Services Basel Regulatory Capital Internal Ratings Based Approach accessible data as well as unauthorized read access to a subset of Oracle Financial Services Basel Regulatory Capital Internal Ratings Based Approach accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity	NA	A-Ora-Finan/16-05-18/9

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-2859**		
Flexcube Core Banking					
NA	18-04-2018	5.8	Vulnerability in the Oracle FLEXCUBE Core Banking component of Oracle Financial Services Applications (subcomponent: Securities). Supported versions that are affected are 11.5.0, 11.6.0 and 11.7.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle FLEXCUBE Core Banking. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle FLEXCUBE Core Banking, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Core Banking accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Core Banking accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-2807**	NA	A-Ora-Flexc/16-05-18/10
Goldengate					
NA	18-04-2018	5	Vulnerability in the Oracle GoldenGate component of	NA	A-Ora-Golde/16-

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			Oracle GoldenGate. The supported version that is affected is 12.2.0.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle GoldenGate. While the vulnerability is in Oracle GoldenGate, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle GoldenGate accessible data. CVSS 3.0 Base Score 8.6 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N). **CVE-ID:CVE-2018-2832**		05-18/11
Hospitality Reporting And Analytics					
NA	18-04-2018	5.5	Vulnerability in the Oracle Hospitality Reporting and Analytics component of Oracle Hospitality Applications (subcomponent: Report). The supported version that is affected is 9.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hospitality Reporting and Analytics. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hospitality Reporting and Analytics accessible data as well as unauthorized access to critical data or complete access	NA	A-Ora-Hospi/16-05-18/12

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			to all Oracle Hospitality Reporting and Analytics accessible data. CVSS 3.0 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). **CVE-ID:CVE-2018-2803**		
Hospitality Suite8					
NA	18-04-2018	6	Vulnerability in the Oracle Hospitality Suite8 component of Oracle Hospitality Applications (subcomponent: Profile). The supported version that is affected is 8.x. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hospitality Suite8. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality Suite8 accessible data as well as unauthorized update, insert or delete access to some of Oracle Hospitality Suite8 accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Hospitality Suite8. CVSS 3.0 Base Score 7.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:L/A:H). **CVE-ID:CVE-2018-2827**	NA	A-Ora-Hospi/16-05-18/13

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
Human Resources					
NA	18-04-2018	6.4	Vulnerability in the Oracle Human Resources component of Oracle E-Business Suite (subcomponent: General Utilities). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Human Resources. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Human Resources accessible data as well as unauthorized access to critical data or complete access to all Oracle Human Resources accessible data. CVSS 3.0 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N). **CVE-ID:CVE-2018-2870**	NA	A-Ora-Human/16-05-18/14
NA	18-04-2018	6.4	Vulnerability in the Oracle Human Resources component of Oracle E-Business Suite (subcomponent: General Utilities). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Human Resources. Successful attacks of this	NA	A-Ora-Human/16-05-18/15

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Human Resources accessible data as well as unauthorized access to critical data or complete access to all Oracle Human Resources accessible data. CVSS 3.0 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N). **CVE-ID:CVE-2018-2871**		
Gain Information	18-04-2018	5	Vulnerability in the Oracle Human Resources component of Oracle E-Business Suite (subcomponent: General Utilities). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Human Resources. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Human Resources accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE-ID:CVE-2018-2868**	NA	A-Ora-Human/16-05-18/16
Gain Information	18-04-2018	5	Vulnerability in the Oracle Human Resources component of Oracle E-Business Suite (subcomponent: General Utilities). Supported versions	NA	A-Ora-Human/16-05-18/17

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Human Resources. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Human Resources accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE-ID:CVE-2018-2869**		
Primavera P6 Enterprise Project Portfolio Management					
NA	18-04-2018	4	Vulnerability in the Primavera P6 Enterprise Project Portfolio Management component of Oracle Construction and Engineering Suite (subcomponent: Web Access). Supported versions that are affected are 16.2 and 17.1 - 17.12. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Primavera P6 Enterprise Project Portfolio Management. While the vulnerability is in Primavera P6 Enterprise Project Portfolio Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Primavera P6 Enterprise	NA	A-Ora-Prima/16-05-18/18

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			Project Portfolio Management accessible data. CVSS 3.0 Base Score 7.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N). **CVE-ID:CVE-2018-2849**		
Retail Back Office					
DoS	18-04-2018	6.4	Vulnerability in the Oracle Retail Back Office component of Oracle Retail Applications (subcomponent: Security). Supported versions that are affected are 13.4.9, 14.0.4 and 14.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Retail Back Office. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Retail Back Office accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Retail Back Office. CVSS 3.0 Base Score 6.5 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L). **CVE-ID:CVE-2018-2861**	NA	A-Ora-Retai/16-05-18/19
Retail Integration Bus					
DoS	18-04-2018	6.8	Vulnerability in the Oracle Retail Integration Bus component of Oracle Retail Applications (subcomponent: RIB Kernal(Apache Commons Collections)). The supported version that is affected is 13.2. Easily exploitable vulnerability	NA	A-Ora-Retai/16-05-18/20

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			allows unauthenticated attacker with network access via HTTP to compromise Oracle Retail Integration Bus. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Retail Integration Bus, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Retail Integration Bus accessible data as well as unauthorized read access to a subset of Oracle Retail Integration Bus accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Retail Integration Bus. CVSS 3.0 Base Score 7.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L). **CVE-ID:CVE-2018-2876**		
Retail Point-of-service					
NA	18-04-2018	5.5	Vulnerability in the Oracle Retail Point-of-Service component of Oracle Retail Applications (subcomponent: User Interface). Supported versions that are affected are 13.3.8, 13.4.9, 14.0.4 and 14.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Retail Point-of-Service. Successful	NA	A-Ora-Retai/16-05-18/21

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Retail Point-of-Service accessible data as well as unauthorized update, insert or delete access to some of Oracle Retail Point-of-Service accessible data. CVSS 3.0 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N). **CVE-ID:CVE-2018-2862**		
Retail Xstore Point Of Service					
DoS	18-04-2018	6.8	Vulnerability in the Oracle Retail Xstore Point of Service component of Oracle Retail Applications (subcomponent: Xstore Office). Supported versions that are affected are 6.5.11, 7.0.6, 7.1.6, 15.0.1 and 16.0.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Retail Xstore Point of Service. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Retail Xstore Point of Service accessible data as well as unauthorized update, insert or delete access to some of Oracle Retail Xstore Point of Service accessible data and unauthorized ability to cause a partial denial of service	NA	A-Ora-Retai/16-05-18/22

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			(partial DOS) of Oracle Retail Xstore Point of Service. CVSS 3.0 Base Score 7.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:L). **CVE-ID:CVE-2018-2840**		
Transportation Management					
NA	18-04-2018	4	Vulnerability in the Oracle Transportation Management component of Oracle Supply Chain Products Suite (subcomponent: Database). The supported version that is affected is 6.4.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Transportation Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Transportation Management accessible data. CVSS 3.0 Base Score 6.5 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N). **CVE-ID:CVE-2018-2823**	NA	A-Ora-Trans/16-05-18/23
Webcenter Content					
DoS	18-04-2018	6	Vulnerability in the Oracle WebCenter Content component of Oracle Fusion Middleware (subcomponent: Content Server). Supported versions that are affected are 11.1.1.9.0, 12.2.1.2.0 and 12.2.1.3.0. Easily exploitable	NA	A-Ora-Webce/16-05-18/24

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebCenter Content accessible data as well as unauthorized update, insert or delete access to some of Oracle WebCenter Content accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle WebCenter Content. CVSS 3.0 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:L). **CVE-ID:CVE-2018-2828**		
Xyhcms Project					
Xyhcms					
CSRF	16-04-2018	6.8	An issue was discovered in XYHCMS 3.5. It has CSRF via an index.php?g=Manage&m=Rbac&a=addUser request, resulting in addition of an account with the administrator role. **CVE-ID:CVE-2018-10127**	https://github.com/gosea/xyhcms/issues/1	A-Xyh-Xyhcm/16-05-18/25
XSS	16-04-2018	4.3	An issue was discovered in XYHCMS 3.5. It has XSS via the test parameter to index.php.	https://github.com/gosea/xyhcms/	A-Xyh-Xyhcm/16-05-18/26

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			CVE-ID:CVE-2018-10128	issues/2	
Application Operating System (Application,OS)					
Oracle,Redhat					
Enterprise Linux Desktop,Enterprise Linux Server,Enterprise Linux Workstation,JDK,JRE					
NA	18-04-2018	5.1	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Hotspot). Supported versions that are affected are Java SE: 6u181, 7u171, 8u162 and 10; Java SE Embedded: 8u161. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 8.3	https://usn.ubuntu.com/3644-1/, https://access.redhat.com/errata/RHSA-2018:1270, https://access.redhat.com/errata/RHSA-2018:1278, https://access.redhat.com/errata/RHSA-2018:1201, https://access.redhat.com/errata/RHSA-2018:1206, https://access.redhat.com/errata/RHSA-2018:1205, https://access.redhat.com/errata/RHSA-2018:1204, https://access.redhat.com/errata/RHSA-2018:1203, https://access.redhat.com/errata/RHSA-2018:1202, https://access.redhat.com/errata/RHSA-2018:1191,	A-Ora-Enter/16-05-18/27

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE-ID:CVE-2018-2814**	https://access.redhat.com/errata/RHSA-2018:1188, https://security.netapp.com/advisory/ntap-20180419-0001/, https://www.debian.org/security/2018/dsa-4185	
Enterprise Linux Desktop,Enterprise Linux Server,Enterprise Linux Workstation,JDK,JRE,Jrockit					
NA	18-04-2018	3.7	Vulnerability in the Java SE, JRockit component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 6u181, 7u171, 8u162, 10 and JRockit: R28.3.17. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Java SE, JRockit executes to compromise Java SE, JRockit. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, JRockit, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without	https://usn.ubuntu.com/3644-1/, https://security.netapp.com/advisory/ntap-20180419-0001/, https://access.redhat.com/errata/RHSA-2018:1278, https://access.redhat.com/errata/RHSA-2018:1206 , https://access.redhat.com/errata/RHSA-2018:1205, https://access.redhat.com/errata/RHSA-2018:1204, https://access.redhat.com/errata/RHSA-2018:1270, https://access.redhat.com/errata/RHSA-2018:1203,	A-Ora-Enter/16-05-18/28

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 7.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE-ID:CVE-2018-2794**	https://access.redhat.com/errata/RHSA-2018:1202, https://access.redhat.com/errata/RHSA-2018:1188, https://access.redhat.com/errata/RHSA-2018:1191, https://access.redhat.com/errata/RHSA-2018:1201, https://www.debian.org/security/2018/dsa-4185	
NA	18-04-2018	4	Vulnerability in the Java SE, JRockit component of Oracle Java SE (subcomponent: RMI). Supported versions that are affected are Java SE: 6u181, 7u171 and 8u162; JRockit: R28.3.17. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, JRockit. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, JRockit accessible data as well as unauthorized read access to a subset of Java SE, JRockit accessible data. Note: This vulnerability can only be exploited by supplying data to APIs in the specified	https://www.debian.org/security/2018/dsa-4185, https://usn.ubuntu.com/3644-1/, https://security.netapp.com/advisory/ntap-20180419-0001/, https://access.redhat.com/errata/RHSA-2018:1278, https://access.redhat.com/errata/RHSA-2018:1206, https://access.redhat.com/errata/RHSA-2018:1205, https://access.red	A-Ora-Enter/16-05-18/29

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.0 Base Score 4.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N). **CVE-ID:CVE-2018-2800**	hat.com/errata/RHSA-2018:1204, https://access.redhat.com/errata/RHSA-2018:1203, https://access.redhat.com/errata/RHSA-2018:1202, https://access.redhat.com/errata/RHSA-2018:1201, https://access.redhat.com/errata/RHSA-2018:1188, https://access.redhat.com/errata/RHSA-2018:1191, https://access.redhat.com/errata/RHSA-2018:1270	
DoS	18-04-2018	5	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: AWT). Supported versions that are affected are Java SE: 6u181, 7u171, 8u162 and 10; Java SE Embedded: 8u161; JRockit: R28.3.17. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service	https://www.debian.org/security/2018/dsa-4185, https://usn.ubuntu.com/3644-1/, https://security.netapp.com/advisory/ntap-20180419-0001/, https://access.redhat.com/errata/RHSA-2018:1278, https://access.redhat.com/errata/R	A-Ora-Enter/16-05-18/30

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			(partial DOS) of Java SE, Java SE Embedded, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE-ID:CVE-2018-2798**	HSA-2018:1206, https://access.redhat.com/errata/RHSA-2018:1205, https://access.redhat.com/errata/RHSA-2018:1204, https://access.redhat.com/errata/RHSA-2018:1203, https://access.redhat.com/errata/RHSA-2018:1202, https://access.redhat.com/errata/RHSA-2018:1201, https://access.redhat.com/errata/RHSA-2018:1188, https://access.redhat.com/errata/RHSA-2018:1191, https://access.redhat.com/errata/RHSA-2018:1270	
DoS	18-04-2018	5	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JAXP). Supported versions that are affected are Java SE: 7u171, 8u162 and 10; Java SE Embedded: 8u161; JRockit: R28.3.17. Easily exploitable vulnerability allows unauthenticated attacker with	https://www.debian.org/security/2018/dsa-4185, https://access.redhat.com/errata/RHSA-2018:1188, https://access.redhat.com/errata/RHSA-2018:1278,	A-Ora-Enter/16-05-18/31

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE-ID:CVE-2018-2799**	https://security.netapp.com/advisory/ntap-20180419-0001/, https://usn.ubuntu.com/3644-1/, https://access.redhat.com/errata/RHSA-2018:1270, https://access.redhat.com/errata/RHSA-2018:1202, https://access.redhat.com/errata/RHSA-2018:1204, https://access.redhat.com/errata/RHSA-2018:1206, https://access.redhat.com/errata/RHSA-2018:1201, https://access.redhat.com/errata/RHSA-2018:1191	
DoS	18-04-2018	5	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JMX). Supported versions that are affected are Java SE: 6u181, 7u171, 8u162 and 10; Java SE Embedded: 8u161; JRockit: R28.3.17. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java	https://access.redhat.com/errata/RHSA-2018:1270, https://www.debian.org/security/2018/dsa-4185, https://usn.ubuntu.com/3644-1/, https://security.netapp.com/advisor	A-Ora-Enter/16-05-18/32

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE-ID:CVE-2018-2797**	y/ntap-20180419-0001/, https://access.redhat.com/errata/RHSA-2018:1278, https://access.redhat.com/errata/RHSA-2018:1206, https://access.redhat.com/errata/RHSA-2018:1205, https://access.redhat.com/errata/RHSA-2018:1204, https://access.redhat.com/errata/RHSA-2018:1203, https://access.redhat.com/errata/RHSA-2018:1202, https://access.redhat.com/errata/RHSA-2018:1201, https://access.redhat.com/errata/RHSA-2018:1188, https://access.redhat.com/errata/RHSA-2018:1191	
DoS	18-04-2018	5	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Security). Supported versions that are	https://www.debian.org/security/2018/dsa-4185, https://access.red	A-Ora-Enter/16-05-18/33

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			affected are Java SE: 6u181, 7u171, 8u162 and 10; Java SE Embedded: 8u161; JRockit: R28.3.17. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE-ID:CVE-2018-2795**	hat.com/errata/RHSA-2018:1206, https://access.redhat.com/errata/RHSA-2018:1270, https://access.redhat.com/errata/RHSA-2018:1278, https://usn.ubuntu.com/3644-1/, https://access.redhat.com/errata/RHSA-2018:1203, https://access.redhat.com/errata/RHSA-2018:1204, https://access.redhat.com/errata/RHSA-2018:1188, https://access.redhat.com/errata/RHSA-2018:1191, https://access.redhat.com/errata/RHSA-2018:1202, https://security.netapp.com/advisory/ntap-20180419-0001/, https://access.redhat.com/errata/RHSA-2018:1201, ' https://access.red	

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
				hat.com/errata/RHSA-2018:1205	
DoS	18-04-2018	5	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Serialization). Supported versions that are affected are Java SE: 6u181, 7u171, 8u162 and 10; Java SE Embedded: 8u161; JRockit: R28.3.17. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE-ID:CVE-2018-2815**	https://access.redhat.com/errata/RHSA-2018:1206, https://www.debian.org/security/2018/dsa-4185, https://usn.ubuntu.com/3644-1/, https://security.netapp.com/advisory/ntap-20180419-0001/, https://access.redhat.com/errata/RHSA-2018:1278, https://access.redhat.com/errata/RHSA-2018:1270, https://access.redhat.com/errata/RHSA-2018:1205, https://access.redhat.com/errata/RHSA-2018:1204, https://access.redhat.com/errata/RHSA-2018:1188, https://access.redhat.com/errata/RHSA-2018:1191, https://access.red	A-Ora-Enter/16-05-18/34

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
				hat.com/errata/RHSA-2018:1202, https://access.redhat.com/errata/RHSA-2018:1201, https://access.redhat.com/errata/RHSA-2018:1203	
Enterprise Linux Server,Enterprise Linux Workstation,JDK,JRE,Jrockit					
NA	18-04-2018	5.8	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 6u181, 7u161 and 8u152; Java SE Embedded: 8u152; JRockit: R28.3.17. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded, JRockit accessible data as well as unauthorized access to critical data or complete access to all Java SE, Java SE Embedded, JRockit accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified	https://usn.ubuntu.com/3644-1/, https://security.netapp.com/advisory/ntap-20180419-0001/, https://access.redhat.com/errata/RHSA-2018:1205, https://access.redhat.com/errata/RHSA-2018:1203	A-Ora-Enter/16-05-18/35

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N). **CVE-ID:CVE-2018-2783**		
DoS	18-04-2018	5	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Concurrency). Supported versions that are affected are Java SE: 7u171, 8u162 and 10; Java SE Embedded: 8u161; JRockit: R28.3.17. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score	https://security.netapp.com/advisory/ntap-20180419-0001/, https://www.debian.org/security/2018/dsa-4185, https://access.redhat.com/errata/RHSA-2018:1201, https://access.redhat.com/errata/RHSA-2018:1202, https://access.redhat.com/errata/RHSA-2018:1204, https://access.redhat.com/errata/RHSA-2018:1270, https://access.redhat.com/errata/RHSA-2018:1278, https://access.redhat.com/errata/RHSA-2018:1191,	A-Ora-Enter/16-05-18/36

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE-ID:CVE-2018-2796**	https://access.redhat.com/errata/RHSA-2018:1206, https://access.redhat.com/errata/RHSA-2018:1188, https://usn.ubuntu.com/3644-1/	
Operating System (OS)					
Qualcomm					
Fsm9055 Firmware,Ipq4019 Firmware,Mdm9206 Firmware,Mdm9607 Firmware,Mdm9615 Firmware,Mdm9625 Firmware,Mdm9635m Firmware,Mdm9640 Firmware,Mdm9645 Firmware,Mdm9650 Firmware,Mdm9655 Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 600 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820 Firmware,Sd 835 Firmware,Sd 845 Firmware,Sd 850 Firmware,Sdx20 Firmware					
Gain Information	18-04-2018	5	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile, Snapdragon Wear, and Small Cell SoC FSM9055, IPQ4019, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 600, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 835, SD 845, SD 850, and SDX20, code to zeroize AES key could be compiled out by compiler which could potentially result in information disclosure. **CVE-ID:CVE-2015-9123**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Fsm90/16-05-18/37

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
Fsm9055 Firmware,Ipq4019 Firmware,Mdm9206 Firmware,Mdm9607 Firmware,Mdm9625 Firmware,Mdm9635m Firmware,Mdm9640 Firmware,Mdm9645 Firmware,Mdm9650 Firmware,Mdm9655 Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 600 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820a Firmware,Sd 820 Firmware,Sd 835 Firmware,Sd 845 Firmware,Sd 850 Firmware,Sdx20 Firmware					
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, Snapdragon Wear, and Small Cell SoC FSM9055, IPQ4019, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 600, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 820A, SD 835, SD 845, SD 850, and SDX20, when an RSA encryption operation is called, the ce_util_to_unsigned_bin is invoked to convert the input buffer to unsigned binary. The ce_util_to_unsigned_bin function, instead of operating on the size of the unsigned character buffer that is passed, operates on the address - i.e. operates on "c" instead of "*c". Decrementing the address to check if it is less than zero means that the operation will always pass, since a pointer will never be less than zero, and may result in a buffer	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Fsm90/16-05-18/38

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			overflow. **CVE-ID:CVE-2015-9138**		
Fsm9055 Firmware,Ipq4019 Firmware,Mdm9206 Firmware,Mdm9607 Firmware,Mdm9625 Firmware,Mdm9635m Firmware,Mdm9640 Firmware,Mdm9645 Firmware,Mdm9650 Firmware,Mdm9655 Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 835 Firmware,Sdx20 Firmware					
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile, Snapdragon Wear, and Small Cell SoC FSM9055, IPQ4019, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 600, SD 615/16/SD 415, SD 617, SD 650/52, SD 800, SD 808, SD 810, SD 835, and SDX20, the reserved memory of TZ subsystem (like TZ apps and some PIL image subsystem) is not cleared after being used. **CVE-ID:CVE-2014-10052**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Fsm90/16-05-18/39
Fsm9055 Firmware,Mdm9206 Firmware,Mdm9607 Firmware,Mdm9625 Firmware,Mdm9635m Firmware,Mdm9640 Firmware,Mdm9645 Firmware,Mdm9650 Firmware,Mdm9655 Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 600 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sdx20 Firmware					
NA	18-04-2018	5	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile, Snapdragon Wear, and Small Cell SoC FSM9055, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650,	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Fsm90/16-05-18/40

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			MDM9655, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 600, SD 615/16/SD 415, SD 617, SD 650/52, SD 800, SD 808, SD 810, and SDX20, unauthorized memory access possible in online memory dump feature. **CVE-ID:CVE-2015-9140**		
Fsm9055 Firmware,Mdm9635m Firmware,Sd 400 Firmware,Sd 800 Firmware					
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Small Cell SoC FSM9055, MDM9635M, SD 400, and SD 800, improper input validation in tzbsocmem can cause privilege escalation. **CVE-ID:CVE-2015-9196**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Fsm90/16-05-18/41
Fsm9055 Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 800 Firmware,Sd 810 Firmware					
NA	18-04-2018	5	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Small Cell SoC FSM9055, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 615/16/SD 415, SD 800, and SD 810, possible arbitrary memory read due to untrusted pointer dereference when handling HLOS controlled values passed to the QSEE syscall helper. **CVE-ID:CVE-2015-9132**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Fsm90/16-05-18/42
Ipq4019 Firmware,Ipq8064 Firmware,Mdm9206 Firmware,Mdm9607 Firmware,Mdm9635m Firmware,Mdm9640 Firmware,Mdm9645 Firmware,Mdm9650 Firmware,Qca4531 Firmware,Qca6174a Firmware,Qca6574au Firmware,Qca6584au Firmware,Qca6584 Firmware,Qca9377 Firmware,Qca9378 Firmware,Qca9379 Firmware,Qca9558 Firmware,Qca9880 Firmware,Qca9886 Firmware,Qca9980 Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 425 Firmware,Sd 625 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820 Firmware,Sdx20 Firmware					

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, QCA4531, QCA6174A, QCA6574AU, QCA6584, QCA6584AU, QCA9377, QCA9378, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 625, SD 808, SD 810, SD 820, and SDX20, while processing firmware image signature, the internal buffer may overflow if the firmware signature size is large. **CVE-ID:CVE-2014-9998**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Ipq40/16-05-18/43
Ipq4019 Firmware,Ipq8064 Firmware,Mdm9206 Firmware,Mdm9607 Firmware,Mdm9640 Firmware,Mdm9650 Firmware,Qca4531 Firmware,Qca6174a Firmware,Qca6574au Firmware,Qca6584au Firmware,Qca6584 Firmware,Qca9377 Firmware,Qca9378 Firmware,Qca9379 Firmware,Qca9558 Firmware,Qca9880 Firmware,Qca9886 Firmware,Qca9980 Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 425 Firmware,Sd 625 Firmware,Sd 810 Firmware,Sd 820 Firmware,Sdx20 Firmware					
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, QCA4531, QCA6174A, QCA6574AU, QCA6584, QCA6584AU, QCA9377, QCA9378, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 625, SD 810, SD 820, and SDX20, integer overflow occurs when the size	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Ipq40/16-05-18/44

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			of the firmware section is incorrectly encoded in the firmware image. **CVE-ID:CVE-2015-9220**		
Ipq4019 Firmware,Mdm9206 Firmware,Mdm9607 Firmware,Mdm9615 Firmware,Mdm9625 Firmware,Mdm9635m Firmware,Mdm9640 Firmware,Mdm9650 Firmware,Mdm9655 Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 820 Firmware,Sdx20 Firmware					
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear IPQ4019, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 615/16/SD 415, SD 820, and SDX20, buffer overflow vulnerability exist in Sahara boot when program header are parsing. **CVE-ID:CVE-2014-10045**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Ipq40/16-05-18/45
Ipq4019 Firmware,Mdm9206 Firmware,Mdm9607 Firmware,Mdm9615 Firmware,Mdm9625 Firmware,Mdm9635m Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 600 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 808 Firmware,Sd 810 Firmware					
Gain Information	18-04-2018	5	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear IPQ4019, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 600, SD 615/16/SD 415, SD 808, and SD 810, processing of TZ application command in tz_apcmd_handler function	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Ipq40/16-05-18/46

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			could lead to potential content disclosure of secure memory. **CVE-ID:CVE-2015-9189**		
Overflow Memory Corruption Bypass	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear IPQ4019, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 600, SD 615/16/SD 415, SD 808, and SD 810, if start_addr + size is too large in boot_clobber_check_local_address_range(), an integer overflow occurs, resulting in clobber protection check being bypassed and SBL memory corruption. **CVE-ID:CVE-2015-9190**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Ipq40/16-05-18/47
Ipq4019 Firmware,Mdm9206 Firmware,Mdm9607 Firmware,Mdm9615 Firmware,Mdm9625 Firmware,Mdm9640 Firmware,Mdm9645 Firmware,Mdm9650 Firmware,Mdm9655 Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 600 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sdx20 Firmware					
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear IPQ4019, MDM9206, MDM9607, MDM9615, MDM9625, MDM9640, MDM9650, MDM9655, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 600, SD 615/16/SD 415, and SDX20, when reading CDT from eMMC with a very large meta offset (>size of default CDT-array compiled in bootloader) for	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Ipq40/16-05-18/48

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			one of the CDBs, a buffer overflow occurs. **CVE-ID:CVE-2015-9143**		
Ipq4019 Firmware,Mdm9206 Firmware,Mdm9607 Firmware,Mdm9625 Firmware,Mdm9635m Firmware,Mdm9640 Firmware,Mdm9645 Firmware,Mdm9650 Firmware,Mdm9655 Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820a Firmware,Sd 820 Firmware,Sd 835 Firmware,Sd 845 Firmware,Sd 850 Firmware,Sdx20 Firmware					
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear IPQ4019, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 820A, SD 835, SD 845, SD 850, and SDX20, integer underflow vulnerability in function qsee_register_log_buff may lead to arbitrary writing of secure memory. **CVE-ID:CVE-2015-9198**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Ipq40/16-05-18/49
Ipq4019 Firmware,Mdm9206 Firmware,Mdm9607 Firmware,Mdm9625 Firmware,Mdm9635m Firmware,Mdm9640 Firmware,Mdm9645 Firmware,Mdm9650 Firmware,Mdm9655 Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sdx20 Firmware					
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear IPQ4019,	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Ipq40/16-05-18/50

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 615/16/SD 415, SD 617, SD 650/52, SD 800, SD 808, SD 810, and SDX20, lack of proper bounds checking may lead to a buffer overflow. **CVE-ID:CVE-2016-10485**		
Ipq4019 Firmware,Mdm9206 Firmware,Mdm9607 Firmware,Mdm9625 Firmware,Mdm9635m Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 600 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware					
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear IPQ4019, MDM9206, MDM9607, MDM9625, MDM9635M, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 600, SD 615/16/SD 415, SD 617, SD 650/52, SD 800, SD 808, and SD 810, in widevine_dash_cmd_handler(), rsp buffers are passed off to widevine commands. These rsp buffers have values in them, such as buffer lengths, that need to be validated to ensure that no buffer overflow/over-reads happen. However, rsp buffers are not always in locked memory, meaning a time-of-check, time-of-use issue can occur where we check that the value is valid, but then a race condition	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Ipq40/16-05-18/51

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			occurs where this memory is swapped out with a different, possibly out of range, value. **CVE-ID:CVE-2015-9157**		
Ipq4019 Firmware,Mdm9206 Firmware,Mdm9607 Firmware,Mdm9635m Firmware,Mdm9640 Firmware,Mdm9645 Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 800 Firmware,Sd 810 Firmware					
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear IPQ4019, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9645, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 615/16/SD 415, SD 800, and SD 810, the function tzbspil_verify_sig() does not strictly check that the pointer to ELF and program headers and hash segment is within secure memory. It only checks that the address is not in non-secure memory. A given address range can overlap with both secure and non-secure regions - hence if such an address is passed in, it would not pass the non-secure range check, and would be considered valid by the function, even though that memory area could be modified by the non-secure side. **CVE-ID:CVE-2015-9208**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Ipq40/16-05-18/52
Ipq4019 Firmware,Mdm9206 Firmware,Mdm9607 Firmware,Mdm9650 Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820a Firmware,Sd 820 Firmware,Sd 835 Firmware,Sd 845 Firmware,Sd 850 Firmware					

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
NA	18-04-2018	5	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear IPQ4019, MDM9206, MDM9607, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 808, SD 810, SD 820, SD 820A, SD 835, SD 845, and SD 850, DRM provisioning mechanisms used in QSEE applications have a feature to prevent further provisioning. This is done by creating an SFS file called 'finalize_proflag.data' at the end of provisioning. When this feature is enabled, provisioning calls check for the existence of the file in order to decide whether to do provisioning or not. Current implementation allows provisioning without sufficient checks. **CVE-ID:CVE-2015-9166**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Ipq40/16-05-18/53
Ipq4019 Firmware,Mdm9206 Firmware,Mdm9607 Firmware,Mdm9650 Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820a Firmware,Sd 820 Firmware,Sd 835 Firmware,Sd 845 Firmware,Sd 850 Firmware					
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear IPQ4019, MDM9206, MDM9607, MDM9650, MSM8909W, SD	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Ipq40/16-05-18/54

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			210/SD 212/SD 205, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 808, SD 810, SD 820, SD 820A, SD 835, SD 845, and SD 850, in a DRM function, a buffer over-read can occur. **CVE-ID:CVE-2015-9153**		
Ipq4019 Firmware,Mdm9206 Firmware,Mdm9607 Firmware,Mdm9650 Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820a Firmware,Sd 820 Firmware,Sd 835 Firmware,Sd 845 Firmware,Sd 850 Firmware					
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear SD 820A, IPQ4019, MDM9206, MDM9607, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 430, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 808, SD 810, SD 820, SD 835, SD 845, SD 450, and SD 850, lack of input validation for message length causes buffer over read in drm_apencapsulate_save_keys. **CVE-ID:CVE-2014-9988**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Ipq40/16-05-18/55
Ipq4019 Firmware,Mdm9206 Firmware,Mdm9607 Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 600 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820a Firmware,Sd 820 Firmware,Sd 835 Firmware					

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear IPQ4019, MDM9206, MDM9607, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 600, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 820A, and SD 835, detection of Error Condition Without Action in Core. **CVE-ID:CVE-2015-9120**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Ipq40/16-05-18/56
Ipq4019 Firmware,Mdm9206 Firmware,Mdm9607 Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 808 Firmware,Sd 810 Firmware					
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear IPQ4019, MDM9206, MDM9607, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 615/16/SD 415, SD 617, SD 650/52, SD 808, and SD 810, incorrect error handling could lead to a double free in QTEE file service API. **CVE-ID:CVE-2015-9165**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Ipq40/16-05-18/57
Ipq4019 Firmware,Mdm9625 Firmware,Mdm9635m Firmware,Mdm9640 Firmware,Mdm9650 Firmware,Mdm9655 Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820a Firmware,Sd 820 Firmware					
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile and Snapdragon Mobile IPQ4019,	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Ipq40/16-05-18/58

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 615/16/SD 415, SD 800, SD 808, SD 810, SD 820, and SD 820A, A non-secure region check is done while registering QSEE buffer address which is passed by HLOS but not while logging in the QSEE buffer, so corruption of dynamically protected secure region can occur if the non-secure buffer is changed between the time it's checked and when it's used. **CVE-ID:CVE-2015-9199**		
Ipq4019 Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 427 Firmware,Sd 430 Firmware,Sd 435 Firmware,Sd 450 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 625 Firmware,Sd 800 Firmware,Sd 810 Firmware,Sd 820a Firmware,Sd 820 Firmware,Sd 835 Firmware					
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile and Snapdragon Mobile IPQ4019, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 800, SD 810, SD 820, SD 820A, SD 835, and Snapdragon_High_Med_2016, modem owned regions are accessible from secure side. **CVE-ID:CVE-2015-9152**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Ipq40/16-05-18/59
Mdm9206 Firmware,Mdm9607 Firmware,Mdm9615 Firmware,Mdm9625 Firmware,Mdm9635m Firmware,Mdm9640 Firmware,Mdm9645 Firmware,Mdm9650 Firmware,Mdm9655 Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 600 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820 Firmware,Sd 835 Firmware,Sd 845 Firmware,Sd 850 Firmware,Sdx20 Firmware					

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
NA	18-04-2018	5	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 600, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 835, SD 845, SD 850, and SDX20, several EFS2 DIAG command handlers are not calling fs_diag_access_check(). **CVE-ID:CVE-2015-9137**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/60
NA	18-04-2018	5	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 600, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 835, SD 845, SD 850, and SDX20, the DIAG-EFS command EFS2_DIAG_DELTREE, which is handled by the function fs_diag_deltree_handler(), is used to delete files and directories only inside the	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/61

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			/public folder. **CVE-ID:CVE-2015-9213**		
Mdm9206 Firmware,Mdm9607 Firmware,Mdm9615 Firmware,Mdm9625 Firmware,Mdm9635m Firmware,Mdm9640 Firmware,Mdm9645 Firmware,Mdm9650 Firmware,Mdm9655 Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820 Firmware,Sd 835 Firmware,Sd 845 Firmware,Sd 850 Firmware,Sdx20 Firmware					
Gain Information	18-04-2018	5	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 835, SD 845, SD 850, and SDX20, sensitive information may be returned to the QMI client as a response. **CVE-ID:CVE-2015-9119**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/62
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820,	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/63

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			SD 835, SD 845, SD 850, and SDX20, buffer overflow vulnerability in RTP during Volte call. **CVE-ID:CVE-2016-10410**		
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 835, SD 845, SD 850, and SDX20, while processing scheduling message information, a buffer overflow can occur. **CVE-ID:CVE-2015-9144**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/64
Mdm9206 Firmware,Mdm9607 Firmware,Mdm9615 Firmware,Mdm9625 Firmware,Mdm9635m Firmware,Mdm9640 Firmware,Mdm9645 Firmware,Mdm9655 Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820 Firmware					
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9655, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 615/16/SD 415, SD 617, SD	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/65

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			650/52, SD 800, SD 808, SD 810, and SD 820, improper input validation can occur while negotiating an SSL handshake. **CVE-ID:CVE-2015-9139**		
Mdm9206 Firmware,Mdm9607 Firmware,Mdm9615 Firmware,Mdm9625 Firmware,Mdm9635m Firmware,Mdm9640 Firmware,Mdm9645 Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 600 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820 Firmware					
NA	18-04-2018	7.8	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 600, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, and SD 820, UE crash is seen due to IPCMem exhaustion, when UDP data is pumped to UE's ULP (UserPlane Location protocol) UDP port 7275. **CVE-ID:CVE-2016-10416**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/66
Mdm9206 Firmware,Mdm9607 Firmware,Mdm9615 Firmware,Mdm9625 Firmware,Mdm9635m Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 600 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 808 Firmware,Sd 810 Firmware					
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9206,	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/67

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			MDM9607, MDM9615, MDM9625, MDM9635M, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 600, SD 615/16/SD 415, SD 625, SD 650/52, SD 808, SD 810, and SD 450, if an incorrect endpoint number or direction is passed, an out of bounds array access may occur in the USB management module. **CVE-ID:CVE-2014-9989**		
Mdm9206 Firmware,Mdm9607 Firmware,Mdm9615 Firmware,Mdm9625 Firmware,Mdm9635m Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 600 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 808 Firmware,Sd 810 Firmware					
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MSM8909W, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 430, SD 600, SD 615/16/SD 415, SD 625, SD 650/52, SD 808, SD 810, and SD 450, lack of input validation could lead to an out of bound array access. **CVE-ID:CVE-2014-9990**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/68
Mdm9206 Firmware,Mdm9607 Firmware,Mdm9615 Firmware,Mdm9635m Firmware,Mdm9640 Firmware,Mdm9645 Firmware,Mdm9650 Firmware,Mdm9655 Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 600 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820 Firmware,Sd 835 Firmware,Sd 845 Firmware,Sd 850 Firmware,Sdx20 Firmware					
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm	https://source.android.com/security/bulletin/2018-	O-Qua-Mdm92/16-05-18/69

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 600, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 835, SD 845, SD 850, and SDX20, there is improper access control in a file storage API. **CVE-ID:CVE-2015-9209**	04-01	
Mdm9206 Firmware,Mdm9607 Firmware,Mdm9615 Firmware,Mdm9635m Firmware,Mdm9640 Firmware,Mdm9645 Firmware,Mdm9650 Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820a Firmware,Sd 820 Firmware,Sd 835 Firmware,Sd 845 Firmware,Sd 850 Firmware,Sdx20 Firmware					
NA	18-04-2018	6.4	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9607, MDM9615, MDM9635M, MDM9640, MDM9645, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 835, SD 845, SD 850, and SDX20, improper ciphersuite validation leads SecSSL accept an unadvertised ciphersuite. **CVE-ID:CVE-2016-10492**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/70

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
Mdm9206 Firmware,Mdm9607 Firmware,Mdm9615 Firmware,Mdm9635m Firmware,Mdm9640 Firmware,Mdm9650 Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 600 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820 Firmware,Sd 835 Firmware,Sdx20 Firmware					
Execute Code	18-04-2018	7.5	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9607, MDM9615, MDM9635M, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 600, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 835, and SDX20, if radish is executed with an interface name set to an invalid interface name, an arbitrary command of 15 characters or less may be executed as a system call. **CVE-ID:CVE-2016-10456**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/71
Mdm9206 Firmware,Mdm9607 Firmware,Mdm9625 Firmware,Mdm9635m Firmware,Mdm9640 Firmware,Mdm9645 Firmware,Mdm9650 Firmware,Mdm9655 Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 600 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820a Firmware,Sd 820 Firmware,Sd 835 Firmware,Sdx20 Firmware					
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear IPQ4019, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655,	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/72

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 600, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 820A, SD 835, and SDX20, integer overflow in tzbsp can lead to privilege escalation. **CVE-ID:CVE-2015-9201**		
Mdm9206 Firmware,Mdm9607 Firmware,Mdm9625 Firmware,Mdm9635m Firmware,Mdm9640 Firmware,Mdm9645 Firmware,Mdm9650 Firmware,Mdm9655 Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820 Firmware,Sd 835 Firmware,Sd 845 Firmware,Sd 850 Firmware,Sdx20 Firmware					
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 835, SD 845, SD 850, and SDX20, during SSL handshake, if RNG function (crypto API) returns error, SSL uses hard-coded random value. **CVE-ID:CVE-2016-10466**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/73
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9607, MDM9625,	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/74

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 835, SD 845, SD 850, and SDX20, while processing downlink information, an assert can be reached. **CVE-ID:CVE-2016-10482**		
Mdm9206 Firmware,Mdm9607 Firmware,Mdm9625 Firmware,Mdm9635m Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 808 Firmware,Sd 810 Firmware					
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9607, MDM9625, MDM9635M, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 625, SD 650/52, SD 808, and SD 810, improper handling of simultaneous interrupt in USB module during USB RESET and EP COMPLETE. **CVE-ID:CVE-2015-9216**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/75
Mdm9206 Firmware,Mdm9607 Firmware,Mdm9625 Firmware,Mdm9640 Firmware,Mdm9645 Firmware,Mdm9650 Firmware,Mdm9655 Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820 Firmware,Sd 835 Firmware,Sd 845 Firmware,Sd 850 Firmware,Sdx20 Firmware					
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/76

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			Snapdragon Wear MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 835, SD 845, SD 850, and SDX20, an integer overflow leading to buffer overflow can occur in a QuRT API function. **CVE-ID:CVE-2016-10491**		
Mdm9206 Firmware,Mdm9607 Firmware,Mdm9635m Firmware,Mdm9640 Firmware,Mdm9645 Firmware,Mdm9650 Firmware,Mdm9655 Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 617 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sdx20 Firmware					
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9607, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 617, SD 650/52, SD 808, SD 810, and SDX20, in a QTEE syscall handler, an untrusted pointer dereference can occur. **CVE-ID:CVE-2015-9191**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/77
Mdm9206 Firmware,Mdm9607 Firmware,Mdm9635m Firmware,Mdm9640 Firmware,Mdm9645 Firmware,Mdm9650 Firmware,Mdm9655 Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sdx20 Firmware					
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9607, MDM9635M,	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/78

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			MDM9640, MDM9645, MDM9650, MDM9655, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, and SDX20, after loading a dynamically loaded code section, I-Cache is not invalidated, which could lead to executing code from stale cache lines. **CVE-ID:CVE-2014-10051**		
Mdm9206 Firmware,Mdm9607 Firmware,Mdm9635m Firmware,Mdm9640 Firmware,Mdm9645 Firmware,Mdm9650 Firmware,Mdm9655 Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 617 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820a Firmware,Sd 820 Firmware,Sd 835 Firmware,Sd 845 Firmware,Sd 850 Firmware,Sdx20 Firmware					
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MDM9206, MDM9607, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 430, SD 450, SD 617, SD 625, SD 650/52, SD 808, SD 810, SD 820, SD 820A, SD 835, SD 845, SD 850, and SDX20, lack of input validation in NPA driver functions leads to null pointer dereference. **CVE-ID:CVE-2015-9145**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/79
Mdm9206 Firmware,Mdm9607 Firmware,Mdm9635m Firmware,Mdm9640 Firmware,Mdm9645 Firmware,Mdm9655 Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820 Firmware,Sd 835 Firmware					
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm	https://source.android.com/security/bulletin/2018-	O-Qua-Mdm92/16-05-18/80

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9607, MDM9635M, MDM9640, MDM9645, MDM9655, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, and SD 835, possible buffer overflow if SIM card sends a response greater than 64KB of data for stream APDU command. **CVE-ID:CVE-2015-9122**	04-01	
Mdm9206 Firmware,Mdm9607 Firmware,Mdm9635m Firmware,Mdm9640 Firmware,Mdm9645 Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 808 Firmware,Sd 810 Firmware					
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9607, MDM9635M, MDM9640, MDM9645, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 615/16/SD 415, SD 617, SD 650/52, SD 808, and SD 810, when enabling XPUs for SMEM partitions, if configuration values are out of range, memory access outside the SMEM may occur and set incorrect XPU configurations. **CVE-ID:CVE-2015-9197**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/81
Mdm9206 Firmware,Mdm9607 Firmware,Mdm9635m Firmware,Mdm9640 Firmware,Mdm9650 Firmware,Msm8909w Firmware,Qca6174a Firmware,Qca6574au Firmware,Qca9377 Firmware,Qca9379 Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 600 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820					

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
Firmware,Sdx20 Firmware					
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MSM8909W, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 400, SD 450, SD 410/12, SD 425, SD 430, SD 600, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, and SDX20, lack of input validation on BT HCI commands processing allows privilege escalation. **CVE-ID:CVE-2014-10054**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/82
Mdm9206 Firmware,Mdm9607 Firmware,Mdm9635m Firmware,Mdm9640 Firmware,Mdm9650 Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820 Firmware,Sd 835 Firmware,Sdx20 Firmware					
NA	18-04-2018	7.2	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 835, and SDX20, privilege escalation may occur due to inherently insecure treatment	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/83

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			of local files. **CVE-ID:CVE-2016-10451**		
Mdm9206 Firmware,Mdm9607 Firmware,Mdm9635m Firmware,Mdm9650 Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820a Firmware,Sd 820 Firmware,Sd 835 Firmware,Sd 845 Firmware,Sd 850 Firmware					
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MDM9206, MDM9607, MDM9635M, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 820A, SD 835, SD 845, and SD 850, integer overflow may occur when values passed from HLOS (graphics driver busy time, and total time) in TZBSGFX_DCVS_UPDATE_ID are very large. **CVE-ID:CVE-2015-9160**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/84
Mdm9206 Firmware,Mdm9607 Firmware,Mdm9635m Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware					
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9607, MDM9635M, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 615/16/SD 415, SD 617, SD 800, SD 808, and SD 810, when	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/85

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			making a high speed Dual Carrier Downlink Data call in a multicell environment, a buffer overflow may occur. **CVE-ID:CVE-2015-9156**		
Overflow Memory Corruption	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9607, MDM9635M, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 615/16/SD 415, SD 617, SD 800, SD 808, and SD 810, in HHO scenarios, during the ACQ procedure, there are possible instances where the search database is incorrectly updated resulting in memory corruption due to buffer overflow. **CVE-ID:CVE-2015-9141**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/86
Mdm9206 Firmware,Mdm9607 Firmware,Mdm9640 Firmware,Mdm9650 Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 600 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820 Firmware,Sd 835 Firmware,Sdx20 Firmware					
DoS	18-04-2018	5	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 600, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 835, and SDX20, dereference of an	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/87

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			invalid input parameter could cause a denial of service. **CVE-ID:CVE-2016-10415**		
Gain Information	18-04-2018	5	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 600, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 835, and SDX20, LocationService is being exported, which is a way for a service to expose its methods to other services. This makes it possible for any other services to import LocationService and call into the exposed method for bringing up a data connection. **CVE-ID:CVE-2014-10062**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/88
Mdm9206 Firmware,Mdm9607 Firmware,Mdm9640 Firmware,Mdm9650 Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 810 Firmware,Sd 820 Firmware,Sd 835 Firmware					
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 625, SD 650/52, SD 800, SD 810, SD 820, and SD 835, in a GNSS API function, a NULL	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/89

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			pointer dereference can occur. **CVE-ID:CVE-2016-10449**		
Mdm9206 Firmware,Mdm9607 Firmware,Mdm9640 Firmware,Mdm9650 Firmware,Qca6174a Firmware,Qca6574au Firmware,Qca9377 Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 425 Firmware,Sd 600 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820 Firmware					
DoS	18-04-2018	7.8	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9607, MDM9640, MDM9650, QCA6174A, QCA6574AU, QCA9377, SD 210/SD 212/SD 205, SD 425, SD 600, SD 650/52, SD 808, SD 810, SD 820, and SDX20, lack of input validation for HCI H4 UART packet ID cause system denial of service. **CVE-ID:CVE-2016-10464**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/90
Mdm9206 Firmware,Mdm9607 Firmware,Mdm9640 Firmware,Mdm9650 Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 600 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820 Firmware,Sd 835 Firmware,Sdx20 Firmware					
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9607, MDM9640, MDM9650, SD 210/SD 212/SD 205, SD 425, SD 430, SD 450, SD 600, SD 625, SD 650/52, SD 808, SD 810, SD 820, SD 835, and SDX20, in pre-auth request, Host driver uses FT IEs sent by the supplicant. A buffer overflow may occur if FT IEs sent by the supplicant are larger than the expected value.**CVE-ID:CVE-2015-9136**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/91
Mdm9206 Firmware,Mdm9607 Firmware,Mdm9650 Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd					

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
415 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 600 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820 Firmware,Sd 835 Firmware,Sdx20 Firmware					
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9607, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 600, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 835, and SDX20, address and size passed to SCM command 'TZ_INFO_GET_SECURE_STATE _LEGACY_ID' from HLOS Kernel were not being checked, so access outside DDR would occur. **CVE-ID:CVE-2016-10472**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/92
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9607, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 600, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 835, and SDX20, while setting the offsets, time-services allows the user to set bases greater than valid base value which will lead to array index out-of-bound. **CVE-ID:CVE-2014-10048**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/93

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9607, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 600, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 835, and SDX20, in a supplementary services function, a buffer overflow can occur. **CVE-ID:CVE-2016-10473**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/94
Mdm9206 Firmware,Mdm9607 Firmware,Mdm9650 Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820 Firmware,Sd 835 Firmware,Sdx20 Firmware					
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9607, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 835, and SDX20, app is requesting more permissions than required. **CVE-ID:CVE-2016-10457**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/95
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9607, MDM9650,	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/96

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 835, and SDX20, missing array index checks on app index in function qcril_uim_clear_encrypted_pin results in accessing addresses outside the bounds of the buffer when app index is too large. **CVE-ID:CVE-2016-10476**		
Overflow Memory Corruption	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9607, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 835, and SDX20, possible memory corruption due to invalid integer overflow checks in exif parsing. **CVE-ID:CVE-2016-10480**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/97
Mdm9206 Firmware,Mdm9607 Firmware,Mdm9650 Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820a Firmware,Sd 820 Firmware,Sd 835 Firmware,Sd 845 Firmware,Sd 850 Firmware					
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MDM9206,	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/98

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			MDM9607, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 820A, SD 835, SD 845, SD 450, and SD 850, buffer overread vulnerability may occur while provisioning a content with a large message. **CVE-ID:CVE-2014-9993**		
Mdm9206 Firmware,Mdm9607 Firmware,Mdm9650 Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 600 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820 Firmware,Sd 835 Firmware,Sdx20 Firmware					
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9607, MDM9650, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 600, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 835, and SDX20, improper offset validation leads to buffer overflow in video parser. **CVE-ID:CVE-2016-10441**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/99
Overflow	18-04-2018	7.1	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9607, MDM9650, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 600, SD 615/16/SD 415, SD 617, SD 625, SD	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/100

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			650/52, SD 800, SD 808, SD 810, SD 820, SD 835, and SDX20, while playing back a .flv clip which doesn't have an inbuilt seek table, a dynamic index table access is out of bounds and leads to crash. **CVE-ID:CVE-2016-10420**		
Mdm9206 Firmware,Mdm9607 Firmware,Mdm9650 Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 820 Firmware,Sd 835 Firmware,Sdx20 Firmware					
NA	18-04-2018	5	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9607, MDM9650, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 625, SD 650/52, SD 820, SD 835, and SDX20, secure UI crash due to uninitialized link list entry in dynamic font module. **CVE-ID:CVE-2016-10447**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/101
Mdm9206 Firmware,Mdm9615 Firmware,Mdm9625 Firmware,Mdm9635m Firmware,Mdm9640 Firmware,Mdm9645 Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 800 Firmware,Sd 810 Firmware,Sd 820 Firmware					
NA	18-04-2018	7.8	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 615/16/SD 415, SD 617, SD 800, SD 810, and SD 820, during a call, memory exhaustion can occur.	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/102

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			CVE-ID:CVE-2016-10459		
Mdm9206 Firmware,Mdm9625 Firmware,Mdm9635m Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 808 Firmware,Sd 810 Firmware					
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9625, MDM9635M, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 615/16/SD 415, SD 450, SD 625, SD 650/52, SD 808, and SD 810, lack of input validation in PRDiagMaintenanceHandler can leads to buffer over read. **CVE-ID:CVE-2014-9997**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/103
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9625, MDM9635M, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 615/16/SD 415, SD 625, SD 650/52, SD 808, SD 810, and SD 450, if a client or host sends more than 16k bytes of USB mass storage transfer, a buffer overflow occurs. **CVE-ID:CVE-2014-9991**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/104
Mdm9206 Firmware,Mdm9650 Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820a Firmware,Sd 820 Firmware,Sd 835 Firmware,Sd 845 Firmware,Sd 850 Firmware					
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm	https://source.android.com/security/bulletin/2018-	O-Qua-Mdm92/16-05-18/105

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MDM9206, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 820A, SD 835, SD 845, and SD 850, lack of input validation could lead to an untrusted pointer dereference in wdash_core_generic_verify(). **CVE-ID:CVE-2015-9175**	04-01	
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MDM9206, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 820A, SD 835, SD 845, and SD 850, lack of input validation in OEMCrypto_GenerateSignature() can cause buffer over read. **CVE-ID:CVE-2015-9182**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/106
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MDM9206, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/107

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			800, SD 808, SD 810, SD 820, SD 820A, SD 835, SD 845, and SD 850, lack of input validation in playready_licacq_process_response() can lead to memory over read. **CVE-ID:CVE-2015-9210**		
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MDM9206, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 615/16/SD 415, SD 450, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 820A, SD 835, SD 845, and SD 850, data access is not properly validated in the Widevine secure application. **CVE-ID:CVE-2014-10053**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/108
NA	18-04-2018	5	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MDM9206, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 820A, SD 835, SD 845, and SD 850, improper input validation could cause a memory overread and cause the app to crash. **CVE-ID:CVE-2015-9193**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/109

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
Gain Information	18-04-2018	5	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MDM9206, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 820A, SD 835, SD 845, and SD 850, in a PlayReady function, information exposure can occur. **CVE-ID:CVE-2015-9163**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/110
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MDM9206, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 820A, SD 835, SD 845, and SD 850, in a crypto API function, a buffer over-read can occur. **CVE-ID:CVE-2015-9177**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/111
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MDM9206, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/112

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 820A, SD 835, SD 845, and SD 850, in a PlayReady API function, a buffer over-read can occur. **CVE-ID:CVE-2015-9186**		
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MDM9206, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 820A, SD 835, SD 845, and SD 850, in a QTEE crypto function, a buffer overflow can occur. **CVE-ID:CVE-2015-9158**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/113
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MDM9206, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 820A, SD 835, SD 845, and SD 850, incorrect offset check in wdash_core_refresh_keys() may lead to a buffer overread. **CVE-ID:CVE-2015-9170**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/114
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm	https://source.android.com/security/bulletin/2018-	O-Qua-Mdm92/16-05-18/115

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MDM9206, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 820A, SD 835, SD 845, and SD 850, lack of input validation in playready_set_domainid could lead to a buffer overread. **CVE-ID:CVE-2015-9203**	04-01	
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MDM9206, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 820A, SD 835, SD 845, and SD 850, lack of input validation OEMCrypto_GetRandom can cause potential buffer overflow. **CVE-ID:CVE-2015-9159**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/116
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MDM9206, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820,	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/117

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			SD 820A, SD 835, SD 845, and SD 850, while provising the Playready module, a buffer overread may occur if the message passed is large. **CVE-ID:CVE-2015-9211**		
Overflow	18-04-2018	5	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MDM9206, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 820A, SD 835, SD 845, and SD 850, Input_address is registered as a shared buffer and is not properly checked before use in OEMCrypto_Generic_Sign(). This allows addresses to be accessed that reside in secure/CP memory. **CVE-ID:CVE-2015-9176**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/118
Mdm9206 Firmware,Mdm9650 Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820a Firmware,Sd 820 Firmware,Sd 835 Firmware,Sdx20 Firmware					
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MDM9206, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/119

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			800, SD 808, SD 810, SD 820, SD 820A, and SD 835, lack of validation of the buffer size could lead to a buffer overread. **CVE-ID:CVE-2015-9128**		
Mdm9206 Firmware,Mdm9650 Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820a Firmware,Sd 820 Firmware,Sd 835 Firmware,Sd 845 Firmware,Sd 850 Firmware					
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MDM9206, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 808, SD 810, SD 820, SD 820A, SD 835, SD 845, and SD 850, if OEMCrypto_Dash_InstallEncapKeybox() is called with keyBoxLength set to a value higher than TZ_WMAX_DATLEN (20k), a buffer over-read occurs. **CVE-ID:CVE-2015-9171**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/120
Mdm9206 Firmware,Mdm9650 Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820a Firmware,Sd 820 Firmware,Sd 835 Firmware,Sd 845 Firmware,Sd 850 Firmware					
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MDM9206, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 430, SD	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/121

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 808, SD 810, SD 820, SD 820A, SD 835, SD 845, and SD 850, if the size parameter passed to TZ_PR_CMD_CONTENT_SET_PROP is small, an integer underflow occurs. **CVE-ID:CVE-2015-9129**		
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MDM9206, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 808, SD 810, SD 820, SD 820A, SD 835, SD 845, and SD 850, while processing the content headers in the Playready module, a buffer overread may occur if the header count exceeds the expected value. **CVE-ID:CVE-2015-9202**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/122
Mdm9206 Firmware,Mdm9650 Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820a Firmware,Sd 820 Firmware,Sd 835 Firmware,Sd 845 Firmware,Sd 850 Firmware					
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MDM9206, MDM9650, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/123

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			808, SD 810, SD 820, SD 820A, SD 835, SD 845, and SD 850, in a DIAG ioctl handler, an untrusted pointer dereference can occur. **CVE-ID:CVE-2015-9149**		
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MDM9206, MDM9650, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 820A, SD 835, SD 845, and SD 850, in a WideVine API function, a buffer over-read can occur. **CVE-ID:CVE-2015-9172**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/124
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MDM9206, MDM9650, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 820A, SD 835, SD 845, and SD 850, out of bounds memory access vulnerability may occur in the content protection manager due to improper validation of incoming messages. **CVE-ID:CVE-2015-9192**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/125

Mdm9206 Firmware,Mdm9650 Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 600 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 625 Firmware,Sd 650

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820a Firmware,Sd 820 Firmware,Sd 835 Firmware,Sd 845 Firmware,Sd 850 Firmware					
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MDM9206, MDM9650, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 430, SD 450, SD 600, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 820A, SD 835, SD 845, and SD 850, the response pointer passed from user space to SDMX_process is not checked before it is used. If the given response buffer length is smaller than 16 bytes, the response values will be written to a memory outside the buffer, possibly in the secure memory area. **CVE-ID:CVE-2015-9180**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/126
Overflow Mem. Corr.	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MDM9206, MDM9650, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 430, SD 450, SD 600, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 820A, SD 835, SD 845, and SD 850, in multiple Secure DEMUX functions (e.g., SDMX_open_session, SDMX_close_session, SDMX_set_session_cfg), when	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/127

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			parameter validation fails, an error code is written into a response buffer, without checking that response buffer length (rsplen) passed from HLOS is large enough to hold the response. If the buffer is at the end of a non-secure page followed by secured memory page, this can cause a secure memory corruption. **CVE-ID:CVE-2015-9185**		
Overflow Mem. Corr.	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MDM9206, MDM9650, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 430, SD 450, SD 600, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 820A, SD 835, SD 845, and SD 850, in Secure DEMUX command handler, when parameter validation fails, an error code is written into a response buffer without checking that response buffer length, passed from HLOS, which may result in memory corruption. **CVE-ID:CVE-2015-9188**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/128
Mdm9206 Firmware,Mdm9650 Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820a Firmware,Sd 820 Firmware,Sd 835 Firmware,Sd 845 Firmware,Sd 850 Firmware					
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/129

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			Snapdragon Wear MDM9206, MDM9650, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 820A, SD 835, SD 845, and SD 850, lack of buffer length validation in pvr_cmd_handler leads to unauthorized access to secure memory. **CVE-ID:CVE-2015-9187**		
Overflow Mem. Corr.	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MDM9206, MDM9650, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 820A, SD 835, SD 845, and SD 850, while processing the rmp secure command, memory corruption may result if the response buffer is smaller than the expected size. **CVE-ID:CVE-2015-9178**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/130
Mdm9206 Firmware,Mdm9650 Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820a Firmware,Sd 820 Firmware,Sd 835 Firmware,Sd 845 Firmware,Sd 850 Firmware					
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MDM9206, MDM9650, SD 210/SD 212/SD	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/131

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			205, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 808, SD 810, SD 820, SD 820A, SD 835, SD 845, and SD 850, a buffer over-read can occur in a DRM API. **CVE-ID:CVE-2014-9987**		
Mdm9206 Firmware,Mdm9650 Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 835 Firmware					
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9650, SD 210/SD 212/SD 205, SD 425, SD 430, SD 450, SD 625, SD 650/52, and SD 835, in some TrustZone API functions, untrusted pointers can be dereferenced. **CVE-ID:CVE-2015-9200**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm92/16-05-18/132
Mdm9607 Firmware,Mdm9635m Firmware,Mdm9640 Firmware,Mdm9645 Firmware,Mdm9650 Firmware,Mdm9655 Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 617 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820 Firmware,Sd 835 Firmware,Sd 845 Firmware,Sd 850 Firmware,Sdx20 Firmware					
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9607, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 430, SD 450, SD 617, SD 625, SD 650/52, SD 808, SD 810, SD 820, SD 835, SD 845, SD 850, and SDX20, possible buffer overflow when processing 1X circuit service message.	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm96/16-05-18/133

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			CVE-ID:CVE-2015-9126		
Mdm9607 Firmware,Mdm9635m Firmware,Mdm9640 Firmware,Mdm9650 Firmware,Qca4531 Firmware,Qca6174a Firmware,Qca6574au Firmware,Qca6584au Firmware,Qca6584 Firmware,Qca9377 Firmware,Qca9378 Firmware,Qca9379 Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 425 Firmware,Sd 600 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820 Firmware,Sd 835 Firmware,Sd 845 Firmware,Sdx20 Firmware					
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, QCA4531, QCA6174A, QCA6574AU, QCA6584, QCA6584AU, QCA9377, QCA9378, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 650/52, SD 808, SD 810, SD 820, SD 835, SD 845, SD 850, and SDX20, if WLAN FW receives the WMI_STSMPS_PARAM_CMDID ioctl in not-associated state, when the virtual channel handle is not assigned, the code doesn't check for NULL virtual channel handle, so an assert occurs. **CVE-ID:CVE-2016-10481**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm96/16-05-18/134
Mdm9615 Firmware,Mdm9625 Firmware,Mdm9635m Firmware,Mdm9640 Firmware,Mdm9650 Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 435 Firmware,Sd 617 Firmware,Sd 625 Firmware					
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, SD 210/SD 212/SD 205, SD 400, SD 425, SD 430, SD 435, SD 617, SD 625, and Snapdragon_High_Med_2016,	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm96/16-05-18/135

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			binary Calibration files under data/misc/audio have 777 permissions. **CVE-ID:CVE-2014-10057**		
Mdm9615 Firmware,Mdm9625 Firmware,Mdm9635m Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware					
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile MDM9615, MDM9625, MDM9635M, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 615/16/SD 415, SD 800, SD 808, and SD 810, use after free vulnerability when the PDN throttle info block is freed without clearing the corresponding active timer. **CVE-ID:CVE-2014-10046**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm96/16-05-18/136
Mdm9615 Firmware,Mdm9625 Firmware,Mdm9635m Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 617 Firmware,Sd 800 Firmware,Sd 820 Firmware					
NA	18-04-2018	5	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile MDM9615, MDM9625, MDM9635M, SD 210/SD 212/SD 205, SD 400, SD 617, SD 800, and SD 820, in the time daemon, unauthorized users can potentially modify system time and cause an array index to be out-of-bound. **CVE-ID:CVE-2014-10044**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm96/16-05-18/137
Mdm9615 Firmware,Mdm9625 Firmware,Mdm9635m Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware					
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile MDM9615, MDM9625, MDM9635M, SD	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm96/16-05-18/138

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			400, SD 410/12, SD 615/16/SD 415, SD 800, SD 808, and SD 810, in ADSP's QDI Root-PD driver, untrusted arguments from User PD may cause integer overflow resulting in buffer overflow. **CVE-ID:CVE-2015-9118**		
Mdm9615 Firmware,Mdm9625 Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 800 Firmware					
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile MDM9615, MDM9625, SD 210/SD 212/SD 205, SD 400, and SD 800, improper access control on ATCMD service allows third party services to access without user knowledge. **CVE-ID:CVE-2014-10059**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm96/16-05-18/139
Mdm9625 Firmware,Mdm9635m Firmware,Mdm9640 Firmware,Mdm9645 Firmware,Mdm9650 Firmware,Mdm9655 Firmware,Sd 400 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 600 Firmware,Sd 617 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820a Firmware,Sd 820 Firmware,Sd 835 Firmware,Sd 845 Firmware,Sd 850 Firmware,Sdx20 Firmware					
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile and Snapdragon Mobile MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, SD 400, SD 425, SD 430, SD 450, SD 600, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 820A, SD 835, SD 845, SD 850, and SDX20, in the Diag User-PD command registration function, a length variable used during buffer allocation is not checked, so if it is very large, an integer overflow followed	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm96/16-05-18/140

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			by a buffer overflow occurs. **CVE-ID:CVE-2015-9148**		
Mdm9625 Firmware,Mdm9635m Firmware,Mdm9640 Firmware,Mdm9645 Firmware,Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware					
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MDM9625, MDM9635M, MDM9640, MDM9645, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 615/16/SD 415, SD 617, SD 650/52, SD 800, SD 808, and SD 810, in a QTEE syscall handler, an untrusted pointer dereference can occur. **CVE-ID:CVE-2015-9135**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm96/16-05-18/141
Mdm9625 Firmware,Mdm9635m Firmware,Mdm9640 Firmware,Mdm9645 Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware					
NA	18-04-2018	8.5	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile MDM9625, MDM9635M, MDM9640, MDM9645, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 615/16/SD 415, SD 800, SD 808, and SD 810, the device may crash while accessing an invalid pointer or expose otherwise inaccessible memory contents. **CVE-ID:CVE-2015-9124**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm96/16-05-18/142
Mdm9625 Firmware,Mdm9635m Firmware,Mdm9650 Firmware,Mdm9655 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sdx20 Firmware					
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm	https://source.android.com/security/bulletin/2018-	O-Qua-Mdm96/16-05-18/143

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			Snapdragon Mobile MDM9625, MDM9635M, MDM9650, MDM9655, SD 400, SD 410/12, SD 615/16/SD 415, SD 617, SD 650/52, SD 808, SD 810, and SDX20, in a QTEE syscall handler, HLOS can cause a buffer overflow to occur. **CVE-ID:CVE-2015-9195**	04-01	
Mdm9625 Firmware,Mdm9635m Firmware,Mdm9650 Firmware,Mdm9655 Firmware,Sd 400 Firmware,Sd 800 Firmware,Sd 835 Firmware,Sd 845 Firmware,Sd 850 Firmware,Sdx20 Firmware					
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile MDM9625, MDM9635M, MDM9645, MDM9650, MDM9655, SD 400, SD 800, SD 835, SD 845, SD 850, and SDX20, when QDI read, write, or ioctl are called, the passed-in pointer is not properly validated before accessing it for the delayed response. **CVE-ID:CVE-2015-9146**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm96/16-05-18/144
Mdm9625 Firmware,Mdm9635m Firmware,Sd 400 Firmware,Sd 800 Firmware					
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile MDM9625, MDM9635M, SD 400, and SD 800, userspace-provided pointer arguments are not validated. **CVE-ID:CVE-2015-9147**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm96/16-05-18/145
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile MDM9625, MDM9635M, SD 400, and SD 800, userspace-provided pointer arguments are not validated. **CVE-ID:CVE-2015-9151**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm96/16-05-18/146

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile MDM9625, MDM9635M, SD 400, and SD 800, while computing the length of memory allocated for a Diag event, if the buffer length is very small or greater than the maximum, an integer overflow may occur, which later results in a buffer overflow. **CVE-ID:CVE-2015-9150**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm96/16-05-18/147
Mdm9625 Firmware,Sd 400 Firmware,Sd 800 Firmware					
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile MDM9625, SD 400, and SD 800, calling qsee_apentry_return() without first calling qsee_apentry() will cause the stack to be restored to an older state resulting in a return to an unexpected location. **CVE-ID:CVE-2014-10039**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm96/16-05-18/148
Mdm9625 Firmware,Sd 400 Firmware,Sd 800 Firmware,Sd 820a Firmware,Sd 820 Firmware					
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile and Snapdragon Mobile MDM9625, SD 400, SD 800, SD 820, and SD 820A, lack of input validation in QSEE can cause potential buffer overflow. **CVE-ID:CVE-2015-9112**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm96/16-05-18/149
Mdm9625 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 820a Firmware,Sd 820 Firmware					
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch	https://source.android.com/security	O-Qua-Mdm96/16-

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			level on Qualcomm Snapdragon Automobile and Snapdragon Mobile MDM9625, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 820, and SD 820A, no address argument validation is performed on calls to the qsee_prng_getdata syscall. **CVE-ID:CVE-2015-9115**	/bulletin/2018-04-01	05-18/150
Mdm9625 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 810 Firmware,Sd 820a Firmware,Sd 820 Firmware					
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile and Snapdragon Mobile MDM9625, SD 425, SD 430, SD 450, SD 625, SD 650/52, SD 810, SD 820, and SD 820A, in a QTEE syscall handler, an untrusted pointer dereference can occur. **CVE-ID:CVE-2015-9116**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm96/16-05-18/151
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile and Snapdragon Mobile MDM9625, SD 425, SD 430, SD 450, SD 625, SD 650/52, SD 810, SD 820, and SD 820A, untrusted pointer dereference in QSEE Syscall without proper validation can lead to access of blacklisted memory. **CVE-ID:CVE-2015-9113**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm96/16-05-18/152
Mdm9625 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 820a Firmware,Sd 820 Firmware					
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile and Snapdragon Mobile MDM9625,	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm96/16-05-18/153

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			SD 425, SD 430, SD 450, SD 625, SD 650/52, SD 820, and SD 820A, in a QTEE syscall handler, an untrusted pointer dereference can occur. **CVE-ID:CVE-2015-9111**		
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile and Snapdragon Mobile MDM9625, SD 425, SD 430, SD 450, SD 625, SD 650/52, SD 820, and SD 820A, lack of address argument validation inqsee_fuse_write could lead to untrusted pointer dereference. **CVE-ID:CVE-2015-9109**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm96/16-05-18/154
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile and Snapdragon Mobile MDM9625, SD 425, SD 430, SD 450, SD 625, SD 650/52, SD 820, and SD 820A, no address argument validation performed on calls to a QSEE syscall may lead to arbitrary read/write or NULL Pointer exception when calling a downstream function. **CVE-ID:CVE-2015-9108**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm96/16-05-18/155
Mdm9625 Firmware,Sd 800 Firmware					
NA	18-04-2018	5	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile MDM9625 and SD 800, a fuse is not correctly blown on a secure device. **CVE-ID:CVE-2014-10063**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm96/16-05-18/156

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
Mdm9635m Firmware,Sd 400 Firmware,Sd 800 Firmware					
Bypass	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile MDM9635M, SD 400, and SD 800, TOCTOU condition may result in bypassing error condition checks, leading to undefined behavior. **CVE-ID:CVE-2014-9985**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm96/16-05-18/157
Mdm9645 Firmware,Mdm9650 Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 427 Firmware,Sd 430 Firmware,Sd 435 Firmware,Sd 450 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820 Firmware,Sdm630 Firmware,Sdm636 Firmware,Sdm660 Firmware					
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile MDM9645, MDM9650, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SDM630, SDM636, SDM660, and Snapdragon_High_Med_2016, bounds check is missing for vtable index in DAL-TO-QDI conversion framework. **CVE-ID:CVE-2015-9142**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Mdm96/16-05-18/158
Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820a Firmware,Sd 820 Firmware					
NA	18-04-2018	5	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MSM8909W, SD 210/SD 212/SD 205, SD 400, SD	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Msm89/16-05-18/159

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, and SD 820A, in playready_licacq_process_response(), 'cbResponse' value is controlled by HLOS, and there is no validation on this length. If 'cbResponse' is too large, memory overread occurs. **CVE-ID:CVE-2014-9986**		
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, and SD 820A, a buffer overread in Playready may occur due to lack of input validation of the buffer size provided by HLOS. **CVE-ID:CVE-2015-9164**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Msm89/16-05-18/160
Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820a Firmware,Sd 820 Firmware,Sd 835 Firmware					
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Msm89/16-05-18/161

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 820A, and SD 835, in a crypto API function, a buffer over-read can occur. **CVE-ID:CVE-2015-9181**		
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile, Snapdragon Mobile, and Snapdragon Wear MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 430, SD 450, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 820A, and SD 835, lack of length checking in wdash_core_load_keys_v8() could lead to a buffer overflow vulnerability. **CVE-ID:CVE-2015-9184**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Msm89/16-05-18/162
Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware					
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 615/16/SD 415, SD 617, SD 650/52, SD 800, SD 808, and SD 810, lack of input validation in playready_getadditional_responsedata could lead to a buffer overread. **CVE-ID:CVE-2015-9207**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Msm89/16-05-18/163

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
Gain Information	18-04-2018	5	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 615/16/SD 415, SD 617, SD 650/52, SD 800, SD 808, and SD 810, buffer over-read in QSEE app may cause confidential information to be leaked. **CVE-ID:CVE-2015-9169**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Msm89/16-05-18/164
Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820 Firmware,Sd 835 Firmware,Sd 845 Firmware,Sd 850 Firmware,Sdx20 Firmware					
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 615/16/SD 415, SD 617, SD 650/52, SD 800, SD 808, and SD 810, TOCTOU condition could lead to a buffer overflow in function playready_reader_bind(). **CVE-ID:CVE-2015-9161**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Msm89/16-05-18/165
Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 808 Firmware,Sd 810 Firmware					
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 615/16/SD 415, SD 617, SD 650/52, SD 808,	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Msm89/16-05-18/166

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			and SD 810, in a PlayReady function, a NULL pointer dereference can occur. **CVE-ID:CVE-2015-9130**		
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 615/16/SD 415, SD 617, SD 650/52, SD 808, and SD 810, during XML encoding of a message in the Playready module, a buffer overread may occur if the message passed is large. **CVE-ID:CVE-2015-9206**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Msm89/16-05-18/167
Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 810 Firmware					
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 615/16/SD 415, and SD 810, possible null pointer dereference occurs due to failure of memory allocation when a large value is passed for buffer allocation in the Playready App. **CVE-ID:CVE-2015-9127**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Msm89/16-05-18/168
Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 425 Firmware,Sd 427 Firmware,Sd 430 Firmware,Sd 435 Firmware,Sd 450 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820 Firmware,Sd 835 Firmware,Sd 845 Firmware,Sdm630 Firmware,Sdm636 Firmware,Sdm660 Firmware					
NA	18-04-2018	4.9	In Android before 2018-04-05 or earlier security patch level on Qualcomm	https://source.android.com/security/bulletin/2018-	O-Qua-Msm89/16-05-18/169

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			Snapdragon Mobile and Snapdragon Wear MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 835, SD 845, SDM630, SDM636, SDM660, and Snapdragon_High_Med_2016, when processing bad HEVC clips, the DPB fills, and with no error handling for DPB being full, a hang occurs. **CVE-ID:CVE-2015-9218**	04-01	
NA	18-04-2018	7.2	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 835, SD 845, SDM630, SDM636, SDM660, and Snapdragon_High_Med_2016, certain malformed HVEC clips could cause an assertion to fail. **CVE-ID:CVE-2015-9217**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Msm89/16-05-18/170
NA	18-04-2018	7.8	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, SD 835, SD 845,	https://source.android.com/security/bulletin/2018-04-01, https://www.exploit-db.com/exploits/39739/	O-Qua-Msm89/16-05-18/171

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			SDM630, SDM636, SDM660, and Snapdragon_High_Med_2016, processing erroneous bitstreams may result in a HW freeze. FW should detect the HW freeze based on watchdog timer, but because the watchdog timer is not enabled, an infinite loop occurs, resulting in a device freeze. **CVE-ID:CVE-2015-9222**		
Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 800 Firmware					
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, and SD 800, lack of input validation while processing TZ_PR_CMD_SAVE_KEY command could lead to a buffer overread. **CVE-ID:CVE-2015-9212**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Msm89/16-05-18/172
Overflow	18-04-2018	5	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, and SD 800, while reading PlayReady rights string information from command buffer (which is sent from non-secure side), if length of rights string is very large, a buffer over read occurs, exposing TZ App memory to non-secure side.	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Msm89/16-05-18/173

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			CVE-ID:CVE-2014-10043		
Msm8909w Firmware,Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 808 Firmware,Sd 810 Firmware					
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MSM8909W, SD 210/SD 212/SD 205, SD 410/12, SD 615/16/SD 415, SD 808, and SD 810, if cchFriendlyName is greater than TZ_PR_MAX_NAME_LEN in function playready_leavedomain_generate_challenge(), a buffer overread occurs. **CVE-ID:CVE-2015-9204**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Msm89/16-05-18/174
Msm8917 Firmware,Msm8939 Firmware,Msm8976 Firmware,Msm8996 Firmware,Sdm660 Firmware,Sdm845 Firmware					
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile MSM8996, MSM8939, MSM8976, MSM8917, SDM845, and SDM660, access control collision vulnerability when accessing the replay protected memory block. **CVE-ID:CVE-2014-10050**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Msm89/16-05-18/175
Msm8974 Firmware					
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile MSM8974, lack of length checking in OEMCrypto_DeriveKeysFromSessionKey() could lead to a buffer overflow vulnerability. **CVE-ID:CVE-2015-9179**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Msm89/16-05-18/176

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware					
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile SD 210/SD 212/SD 205, A buffer overflow can potentially occur in any OpenCL application that calls clBuildProgram() with a device of type CL_DEVICE_TYPE_CPU in its device_list argument. **CVE-ID:CVE-2014-10056**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Sd/16-05-18/177
Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 400 Firmware,Sd 425 Firmware,Sd 427 Firmware,Sd 430 Firmware,Sd 435 Firmware,Sd 450 Firmware,Sd 617 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 845 Firmware					
NA	18-04-2018	5	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile SD 210/SD 212/SD 205, SD 400, SD 425, SD 427, SD 430, SD 435, SD 450, SD 617, SD 625, SD 650/52, SD 800, SD 845, and Snapdragon_High_Med_2016, unauthorized users can potentially modify system time. **CVE-ID:CVE-2014-10058**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Sd/16-05-18/178
Gain Information	18-04-2018	5	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile SD 210/SD 212/SD 205, SD 400, SD 425, SD 427, SD 430, SD 435, SD 450, SD 617, SD 625, SD 650/52, SD 800, SD 845, and Snapdragon_High_Med_2016, during module load at TZ Startup, memory statically allocated by modules was not being properly set to zero first. Allowing the module to execute without reset gives it access to information from	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Sd/16-05-18/179

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			previous app thus leading to information exposure. **CVE-ID:CVE-2015-9194**		
Sd 205 Firmware,Sd 210 Firmware,Sd 212 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 808 Firmware,Sd 810 Firmware					
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear MSM8909W, SD 210/SD 212/SD 205, SD 410/12, SD 615/16/SD 415, SD 808, and SD 810, in a PlayReady API function, a buffer over-read can occur. **CVE-ID:CVE-2015-9205**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Sd/16-05-18/180
Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware					
NA	18-04-2018	5	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile SD 400, SD 410/12, SD 615/16/SD 415, SD 800, SD 808, and SD 810, lack of input validation in qsee can lead to unauthorized memory access. **CVE-ID:CVE-2015-9131**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Sd/16-05-18/181
Sd 400 Firmware,Sd 410 Firmware,Sd 412 Firmware,Sd 617 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 810 Firmware					
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile SD 400, SD 410/12, SD 617, SD 650/52, SD 800, and SD 810, if Widevine App TZ_WCMD_DECRYPT_VIDEO is called with a size too large, an integer overflow may occur. **CVE-ID:CVE-2015-9133**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Sd/16-05-18/182

CV Scoring Scale (CVSS)	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
Sd 400 Firmware,Sd 800 Firmware					
Gain Information	18-04-2018	5	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile SD 400 and SD 800, there could be leakage of protected contents if HLOS doesn't request for security restoration for OCMEM xPU's. **CVE-ID:CVE-2014-10055**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Sd/16-05-18/183
Gain Information	18-04-2018	5	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile SD 400 and SD 800, when writing the Full Disk Encryption key to crypto engine, information leak could occur. **CVE-ID:CVE-2014-10047**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Sd/16-05-18/184
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile SD 400 and SD 800, in drmprocmd_verify_key(), the variable feature_name_length is not validated. There is a check for feature_name_len + filePathLen but there might be an integer wrap when checking feature_name_len + filePathLen. This leads to a buffer overflow. **CVE-ID:CVE-2014-9995**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Sd/16-05-18/185
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile SD 400 and SD 800, lack of validation of input could cause a integer overflow that could subsequently lead to a buffer overflow.	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Sd/16-05-18/186

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			CVE-ID:CVE-2014-9994		
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile SD 400 and SD 800, while verifying provisioning, a buffer overflow can occur. **CVE-ID:CVE-2014-9996**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Sd/16-05-18/187
Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 600 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 617 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware,Sd 820a Firmware,Sd 820 Firmware					
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile and Snapdragon Mobile SD 410/12, SD 425, SD 430, SD 450, SD 600, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, and SD 820A, in an EMM command, an integer underflow can occur. **CVE-ID:CVE-2015-9167**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Sd/16-05-18/188
Sd 410 Firmware,Sd 412 Firmware,Sd 415 Firmware,Sd 615 Firmware,Sd 616 Firmware,Sd 810 Firmware					
NA	18-04-2018	5	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile SD 410/12, SD 615/16/SD 415, and SD 810, while processing QSEE Syscall 'qsee_macc_gen_ecc_privkey', untrusted pointer dereference occurs, which could result in arbitrary write. **CVE-ID:CVE-2015-9134**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Sd/16-05-18/189
Sd 410 Firmware,Sd 412 Firmware,Sd 617 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 800 Firmware,Sd 808 Firmware,Sd 810 Firmware					

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile SD 410/12, SD 617, SD 650/52, SD 800, SD 808, and SD 810, in the function "Certificate_CreateWithBuffer" in the QSEE app TQS, in case of memory allocation failure, we free the memory and return the pointer without setting it to NULL. **CVE-ID:CVE-2015-9162**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Sd/16-05-18/190
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile SD 410/12, SD 617, SD 650/52, SD 800, SD 808, and SD 810, in TQS QSEE application, while parsing "Set Certificates" command an integer overflow may result in buffer overflow. **CVE-ID:CVE-2015-9183**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Sd/16-05-18/191
Overflow	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile SD 410/12, SD 617, SD 650/52, SD 800, SD 808, and SD 810, lack of validation of the return value prior to using for buffer allocation in QSEE application, TQS, may result in memory overwrite. **CVE-ID:CVE-2015-9174**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Sd/16-05-18/192
Overflow Mem. Corr.	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile SD 410/12, SD 617, SD 650/52, SD 800, SD 808, and SD 810, missing of return value check	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Sd/16-05-18/193

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSSS	Description & CV ID	Reference/Patch	NCIIPC ID
			in memscpy can cause memory corruption in TQS App. **CVE-ID:CVE-2015-9173**		
Sd 425 Firmware,Sd 430 Firmware,Sd 450 Firmware,Sd 625 Firmware,Sd 650 Firmware,Sd 652 Firmware,Sd 820a Firmware,Sd 820 Firmware					
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile and Snapdragon Mobile SD 425, SD 430, SD 450, SD 625, SD 650/52, SD 820, and SD 820A, an unsigned RTIC health report susceptible to tampering by malware executing in the context of the HLOS may be requested. **CVE-ID:CVE-2016-10471**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Sd/16-05-18/194
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile and Snapdragon Mobile SD 425, SD 430, SD 450, SD 625, SD 650/52, SD 820, and SD 820A, lack of address argument validation in qsee_query_counter syscall could lead to untrusted pointer dereference. **CVE-ID:CVE-2015-9114**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Sd/16-05-18/195
NA	18-04-2018	10	In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile and Snapdragon Mobile SD 425, SD 430, SD 450, SD 625, SD 650/52, SD 820, and SD 820A, no address argument validation is performed on calls to the qsee_get_secure_state syscall. **CVE-ID:CVE-2015-9110**	https://source.android.com/security/bulletin/2018-04-01	O-Qua-Sd/16-05-18/196

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;