Vulnerability Type(s)	Publish Date	CVSS	Description & CVE-ID	Reference/Patch	NCIIPC ID
Application					
Oracle					
JDK,JRE,Jrockit					
DoS	18-07-2018	4.3	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Concurrency). Supported versions that are affected are Java SE: 6u191, 7u181, 8u172 and 10.0.1; Java SE Embedded: 8u171; JRockit: R28.3.18. 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 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 3.7 (Availability impacts). CVSS Vector:(CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).	https://usn.ubuntu.com/3735-1/ https://security.netapp.com/advisory/ntap-20180726-0001/ https://access.redhat.com/errata/RHSA-2018:2286 https://access.redhat.com/errata/RHSA-2018:2254 https://access.redhat.com/errata/RHSA-2018:2255 https://www.debian.org/security/2018/dsa-4268 https://access.redhat.com/errata/RHSA-2018:2283 https://access.redhat.com/errata/RHSA-2018:2241 https://access.redhat.com/errata/RHSA-2018:2256 https://access.redhat.com/errata/RHSA-2018:2253 https://access.redhat.com/errata/RHSA-2018:2242 https://usn.ubuntu.com/3734-1/	**A-Ora-JDK,J/20-08-18/1**

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	CVSS	Description & CVE-ID	Reference/Patch	NCIIPC ID
			CVE-ID:CVE-2018-2952		
Mysql					
NA	18-07-2018	3.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Encryption). Supported versions that are affected are 5.5.60 and prior, 5.6.40 and prior and 5.7.22 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector:(CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N). **CVE-ID:CVE-2018-2767**	https://usn.ubuntu.com/3725-1/ https://usn.ubuntu.com/3725-2/ https://access.redhat.com/errata/RHSA-2018:2439 https://security.netapp.com/advisory/ntap-20180726-0002/	**A-Ora-Mysql/20-08-18/2**
Weblogic Server					
NA	18-07-2018	7.5	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS - Web Services). Supported versions that are affected are 12.1.3.0, 12.2.1.2 and 12.2.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and	NA	**A-Ora-Weblo/20-08-18/3**

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	CVSS	Description & CVE-ID	Reference/Patch	NCIIPC ID
			Availability impacts). CVSS Vector:(CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE-ID:CVE-2018-2894**		
Hardware					
Intel					
Core I3,Core I5,Core I7,Core M,Core M3,Core M5,Core M7,Xeon					
Gain Information	14-08-2018	4.7	Systems with microprocessors utilizing speculative execution and address translations may allow unauthorized disclosure of information residing in the L1 data cache to an attacker with local user access via a terminal page fault and a side-channel analysis. **CVE-ID:CVE-2018-3620**	https://www.synology.com/support/security/Synology_SA_18_45 https://www.kb.cert.org/vuls/id/982149 https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00161.html https://usn.ubuntu.com/3742-2/ https://www.debian.org/security/2018/dsa-4274 https://usn.ubuntu.com/3741-1/ https://usn.ubuntu.com/3742-1/ https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180814-cpusidechannel https://usn.ubuntu.com/3740-1/ https://usn.ubuntu.com/3740-2/ https://security.netapp.com/advisory/ntap-20180815-0001/	**H-Int-Core/20-08-18/4**

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	CVSS	Description & CVE-ID	Reference/Patch	NCIIPC ID
				https://software.intel.com/security-software-guidance/software-guidance/l1-terminal-fault https://support.f5.com/csp/article/K95275140 https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03874en_us https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2018-0009 https://security.FreeBSD.org/advisories/FreeBSD-SA-18:09.l1tf.asc https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/XRFKQWYV2H4BV75CUNGCGE5TNVQCLBGZ/ https://foreshadowattack.eu/ https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/V4UWGORQWCENCIF2BHWUEF2ODBV75QS2/ https://access.redhat.com/errata/RHS	

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	CVSS	Description & CVE-ID	Reference/Patch	NCIIPC ID
				A-2018:2384 https://access.redhat.com/errata/RHSA-2018:2387 https://access.redhat.com/errata/RHSA-2018:2388 https://access.redhat.com/errata/RHSA-2018:2389 https://access.redhat.com/errata/RHSA-2018:2390 https://access.redhat.com/errata/RHSA-2018:2391 https://access.redhat.com/errata/RHSA-2018:2392 https://access.redhat.com/errata/RHSA-2018:2393 https://access.redhat.com/errata/RHSA-2018:2394 https://access.redhat.com/errata/RHSA-2018:2395 https://access.redhat.com/errata/RHSA-2018:2396 https://access.redhat.com/errata/RHSA-2018:2402 https://access.redhat.com/errata/RHSA-2018:2403 https://access.redhat.com/errata/RHSA-2018:2404	

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	CVSS	Description & CVE-ID	Reference/Patch	NCIIPC ID
Gain Information	14-08-2018	4.7	Systems with microprocessors utilizing speculative execution and address translations may allow unauthorized disclosure of information residing in the L1 data cache to an attacker with local user access with guest OS privilege via a terminal page fault and a side-channel analysis. **CVE-ID:CVE-2018-3646**	https://www.synology.com/support/security/Synology_SA_18_45 https://www.kb.cert.org/vuls/id/982149 https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00161.html https://usn.ubuntu.com/3742-2/ https://www.debian.org/security/2018/dsa-4274 https://usn.ubuntu.com/3741-1/ https://usn.ubuntu.com/3742-1/ https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180814-cpusidechannel https://usn.ubuntu.com/3740-1/ https://usn.ubuntu.com/3740-2/ https://security.netapp.com/advisory/ntap-20180815-0001/ https://software.intel.com/security-software-guidance/software-guidance/l1-terminal-fault https://support.f5.com/csp/article/K31	**H-Int-Core/20-08-18/5**

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	CVSS	Description & CVE-ID	Reference/Patch	NCIIPC ID
				300402 https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03874en_us https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2018-0010 https://security.FreeBSD.org/advisories/FreeBSD-SA-18:09.l1tf.asc https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/XRFKQWYV2H4BV75CUNGCGE5TNVQCLBGZ/ https://foreshadowattack.eu/ https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/V4UWGORQWCENCIF2BHWUEF2ODBV75QS2/ https://access.redhat.com/errata/RHSA-2018:2384 https://access.redhat.com/errata/RHSA-2018:2387 https://access.redhat.com/errata/RHSA-2018:2388 https://access.redh	

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	CVSS	Description & CVE-ID	Reference/Patch	NCIIPC ID
				at.com/errata/RHSA-2018:2389 https://access.redhat.com/errata/RHSA-2018:2390 https://access.redhat.com/errata/RHSA-2018:2391 https://access.redhat.com/errata/RHSA-2018:2392 https://access.redhat.com/errata/RHSA-2018:2393 https://access.redhat.com/errata/RHSA-2018:2394 https://access.redhat.com/errata/RHSA-2018:2395 https://access.redhat.com/errata/RHSA-2018:2396 https://access.redhat.com/errata/RHSA-2018:2402 https://access.redhat.com/errata/RHSA-2018:2403 https://access.redhat.com/errata/RHSA-2018:2404	
Core I3,Core I5,Core I7,Xeon E3					
Gain Information	14-08-2018	5.4	Systems with microprocessors utilizing speculative execution and Intel software guard extensions (Intel SGX) may allow unauthorized disclosure of information residing in the L1 data cache from an enclave to an attacker with local user access via a side-channel analysis. **CVE-ID:CVE-2018-**	https://www.kb.cert.org/vuls/id/982149 https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00161.html https://tools.cisco.com/security/center	**H-Int-Core/20-08-18/6**

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	CVSS	Description & CVE-ID	Reference/Patch	NCIIPC ID
			3615	/content/CiscoSecurityAdvisory/cisco-sa-20180814-cpusidechannel https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2018-0008 https://security.netapp.com/advisory/ntap-20180815-0001/ https://software.intel.com/security-software-guidance/software-guidance/l1-terminal-fault https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03874en_us https://support.f5.com/csp/article/K35558453 https://foreshadowattack.eu/ https://www.synology.com/support/security/Synology_SA_18_45	
Operating System (OS)					
Oracle					
Solaris					
NA	18-07-2018	7.2	Vulnerability in the Solaris component of Oracle Sun Systems Products Suite (subcomponent: Availability Suite Service). Supported versions that are affected are	https://www.exploit-db.com/exploits/45126/	**O-Ora-Solar/20-08-18/7**

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	CVSS	Description & CVE-ID	Reference/Patch	NCIIPC ID
			10 and 11.3. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Solaris executes to compromise Solaris. Successful attacks of this vulnerability can result in takeover of Solaris. CVSS 3.0 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). **CVE-ID:CVE-2018-2892**		