Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
Hardware					
Intel					
Core I3;Core I5;Core I7;Core M;Core M3;Core M5;Core M7;Xeon					
Gain Information	2018-08-14	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://usn.ubuntu.com/3756-1/ https://www.kb.cert.org/vuls/id/982149 https://www.debian.org/security/2018/dsa-4279 https://www.debian.org/security/2018/dsa-4274 https://usn.ubuntu.com/3742-2/ https://usn.ubuntu.com/3742-1/ https://usn.ubuntu.com/3741-2/ https://usn.ubuntu.com/3741-1/ https://usn.ubuntu.com/3740-2/ https://usn.ubuntu.com/3740-1/ https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180814-cpusidechannel https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03874en_us https://support.f5.com/csp/article/K31300402 https://software.intel.	H-INT-CORE - 10918/1

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
				com/security-software-guidance/software-guidance/l1-terminal-fault https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2018-0010 https://security.FreeBSD.org/advisories/FreeBSD-SA-18:09.l1tf.asc https://security.netapp.com/advisory/ntap-20180815-0001/ https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180018 https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/XRFKQWYV2H4BV75CUNGCGE5TNVQCLBGZ/ 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.redhat.com/errata/RHSA-2018:2389 https://access.redhat.com/errata/RHSA-2018:2390 https://access.redhat.com/errata/RHSA-	

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
				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 https://access.redhat.com/errata/RHSA-2018:2602 https://access.redhat.com/errata/RHSA-2018:2603 https://lists.debian.org/debian-lts-announce/2018/08/msg00029.html https://foreshadowattack.eu/ https://www.synology.com/support/security/Synology_S18_45 https://lists.fedoraproject.org/archives/list/package-announce@lists.fedora	

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
				project.org/message/V4UWGORQWCENCIF2BHWUEF2ODBV75QS2/ https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00161.html	
Gain Information	2018-08-14	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://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.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-	H-INT-CORE - 10918/2

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
				2018:2402 https://access.redhat.com/errata/RHSA-2018:2403 https://access.redhat.com/errata/RHSA-2018:2404 https://access.redhat.com/errata/RHSA-2018:2602 https://access.redhat.com/errata/RHSA-2018:2603 https://foreshadowattack.eu/ https://lists.debian.org/debian-lts-announce/2018/08/msg00029.html https://www.synology.com/support/security/Synology_S18_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://www.debian.org/security/2018/dsa-4279 https://www.debian.org/security/2018/dsa-4274 https://usn.ubuntu.com/3742-2/ https://usn.ubuntu.com/3742-1/ https://usn.ubuntu.com/3741-2/ https://usn.ubuntu.com/3740-2/ https://usn.ubuntu.co	

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
				m/3741-1/ https://security.netapp.com/advisory/ntap-20180815-0001/ https://usn.ubuntu.com/3740-1/ https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180814-cpusidechannel https://support.f5.com/csp/article/K95275140 https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03874en_us https://software.intel.com/security-software-guidance/software-guidance/l1-terminal-fault https://security.FreeBSD.org/advisories/FreeBSD-SA-18:09.l1tf.asc https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2018-0009 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180018 https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/XRFKQWYV2H4BV75CU	

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
				NGCGE5TNVQCLBGZ/ https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/V4UWGORQWCENCIF2BHWUEF2ODBV75QS2/	
Core I3,Core I5,Core I7,Xeon E3					
Gain Information	2018-08-14	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-2018-3615**	https://www.kb.cert.org/vuls/id/982149 https://www.synology.com/support/security/Synology_S18_45 https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00161.html https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180814-cpusidechannel https://software.intel.com/security-software-guidance/software-guidance/l1-terminal-fault https://support.f5.com/csp/article/K35558453 https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03874en_us https://security.netapp.com/advisory/ntap-20180815-0001/ https://foreshadowatt	H-INT-CORE - 10918/3

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
				ack.eu/ https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2018-0008	
(Operating System) OS					
Microsoft					
Windows 10;Windows 7;Windows 8.1;Windows Rt 8.1;Windows Server 2008;Windows Server 2012; Windows Server 2016					
NA	2018-08-15	6.9	An elevation of privilege vulnerability exists in the Network Driver Interface Specification (NDIS) when ndis.sys fails to check the length of a buffer prior to copying memory to it, aka "Windows NDIS Elevation of Privilege Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-8342. **CVE ID : CVE-2018-8343**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8343	O-MIC-WINDO-10918/4
NA	2018-08-15	6.9	An elevation of privilege vulnerability exists in the Windows Installer when the Windows Installer fails to properly sanitize input leading to an insecure library loading behavior, aka "Windows Installer Elevation of Privilege Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. **CVE ID : CVE-2018-8339**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8339	O-MIC-WINDO-10918/5
NA	2018-08-15	7.2	An elevation of privilege	https://portal.msrc.mi	O-MIC-

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
			vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka "Win32k Elevation of Privilege Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-8399. **CVE ID : CVE-2018-8404**	crosoft.com/en-US/security-guidance/advisory/CVE-2018-8404	WINDO-10918/6
Execute Code	2018-08-15	7.6	A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed, aka "LNK Remote Code Execution Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-8346. **CVE ID : CVE-2018-8345**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8345	O-MIC-WINDO-10918/7
Execute Code	2018-08-15	9.3	A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka "Microsoft Graphics Remote Code Execution Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. **CVE ID : CVE-2018-8344**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8344	O-MIC-WINDO-10918/8

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;