PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
Apple tvOS <13 Remote DoS or Code Execution Vulnerability in Foundation - CVE-2019-8746	Apple tvOS before 13 is prone to a denial of service or remote code execution vulnerability in Foundation due to out-of-bound memory read. A remote attacker could exploit this issue to crush the system or execute arbitrary code on the affected system.	<13	Vendor - Apple CVE Id - SBV-109360 CVSS Base - 9.8 Reporting Date - 10/29/2019 Vendor's Advisory - https://support.apple.com/en-us/HT210604
Apple MacOS X <10.15.1 Code Execution Vulnerability in AppleGraphicsControl - CVE-2019-8716, CVE-2019-8715	Apple MacOS X before 10.15.1 is prone to a code execution vulnerability in AppleGraphicsControl due to a memory corruption issue. An attacker could exploit this issue to execute arbitrary code with kernel privileges on the affected system via a crafted application.	<10.15.1	Vendor - Apple CVE Id - SBV-109172, SBV-109171 CVSS Base - 9.8 Reporting Date - 10/29/2019 Vendor's Advisory - https://support.apple.com/en-us/HT210722
Trend Micro ATTK Remote Code Execution Vulnerability via System File Spoofing - CVE-2019-9491	Trend Micro Anti-Threat Toolkit (ATTK) versions 1.62.0.1218 and below have a vulnerability that may allow an attacker to place malicious files in the same directory, potentially leading to arbitrary remote code execution (RCE) when executed.	<=1.62.0.1218	Vendor - Trend Micro CVE Id - SBV-108927 CVSS Base - 7.8 Reporting Date - 10/29/2019 Vendor's Advisory - https://success.trendmicro.com/solution/000149878
[cpuoct2019-5072832-NoSQL-Database] Oracle NoSQL Database Remote Unspecified Vulnerability in NoSQL (jackson-databind) - CVE-2018-19362, CVE-2018-19361, CVE-2018-19360 CVE-2018-1936	Oracle NoSQL Database versions prior to 19.3.12, might allow attackers to have unspecified impact by leveraging failure to block the jboss-common-core class from polymorphic deserialization.	<19.3.12	Vendor - Oracle CVE Id - SBV-108795, SBV-108794, SBV-108793 CVSS Base - 9.8 Reporting Date - 10/15/2019 Vendor's Advisory - http://www.oracle.com/technetwork/topics/security/cpuoct2019-5072832.html
[cpuoct2019-5072832-Systems] Oracle Fujitsu Servers Remote DoS or Other Vulnerability in cURL - CVE-2018-1000120	A buffer overflow exists in curl, as used in Oracle XCP firmware prior to 2361 or 3070, running on Fujitsu M10-1, M10-4, M10-4S, M12-1, M12-2, M12-2S servers, in the FTP URL handling that allows an attacker to cause a denial of service or worse.		Vendor - Oracle CVE Id - SSBV-108651 CVSS Base - 9.8 Reporting Date - 10/15/2019 Vendor's Advisory - http://www.oracle.com/technetwork/topics/security/cpuoct2019-5072832.html
[APSB19-49] Adobe Acrobat and Reader Remote Code Execution due to a Heap Overflow Vulnerability - CVE-2019-8197, CVE-2019-8162, CVE-2019-8200, CVE-2019-8169, CVE-2019-8167	Adobe Acrobat DC Continuous through 2019.021.20040, Acrobat Reader DC Continuous through 2019.021.20040, Acrobat 2017 Classic through 2017.011.30148, Acrobat Reader 2017 Classic through 2017.011.30148, Acrobat Classic through 2015.006.30503 and Acrobat Reader through 2015.006.30503 are prone to remote code execution due to a heap overflow.		Vendor - Adobe CVE Id - SBV-108687, SBV-108679, SBV-108668, SBV-108674, CVSS Base - 9.8 Reporting Date - 10/15/2019 Vendor's Advisory - https://helpx.adobe.com/security/products/acrobat/apsb19-49.html
[cpuoct2019-5072832-PeopleSoft] Oracle PeopleSoft Enterprise PeopleTools Remote Out-of-Bounds Read Vulnerability in libssh2 - CVE-2019-3859, CVE-2019-3850, CVE-2019-3861, CVE-2019-3862, CVE-2019-3858	An out of bounds read flaw was discovered in libssh2, as used in Oracle PeopleSoft Enterprise PeopleTools 8.56 and 8.57, in the _libssh2_packet_require and _libssh2_packet_requirev functions. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory.	8.57.8.56	Vendor - Oracle CVE Id - SBV-108545, SBV-108546, SBV-108547, SBV-108544 CVSS Base - 9.1 Reporting Date - 10/15/2019 Vendor's Advisory - http://www.oracle.com/technetwork/topics/security/cpuoct2019-5072832.html
[MS19-OCT] Azure Stack Remote Code Execution Vulnerability - CVE-2019-1372	Azure Stack before 1.7 does not properly check the length of a buffer prior to copying memory to it, making it prone to a remote code execution vulnerability. A remote attacker could exploit this issue to make an unprivileged function run by the user execute code in the context of NT AUTHORITY\system, escaping the Sandbox.	<1.7	Vendor - Microsoft CVE Id - SBV-108124 CVSS Base - 9.6 Reporting Date - 10/08/2019 Vendor's Advisory - https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-1372
SAP Landscape Management Remote Information Disclosure Vulnerability - CVE-2019-0380	Under certain conditions, SAP Landscape Management enterprise edition, version 3.0, allows custom secure parameters default values to be part of the application logs leading to Information Disclosure.	3.0 Enterprise	Vendor - SAP CVE Id - SBV-108300 CVSS Base - 9.1 Reporting Date - 10/08/2019 Vendor's Advisory - https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=528123050
B2B Add-On for SAP NetWeaver Process Integration Remote Security Bypass Vulnerability - CVE-2019-0379	SAP Process Integration, business-to-business add-on, versions 1.0, 2.0, does not perform authentication check properly when the default security provider is changed to BouncyCastle (BC), leading to a Missing Authentication Check.	1.0, 2.0	Vendor - SAP CVE Id - SBV-108299 CVSS Base - 9.3 Reporting Date - 10/08/2019 Vendor's Advisory - https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=528123050
Linux Kernel 5.3.2 and Earlier Buffer Overflow Vulnerability - CVE-2019-17133	In the Linux kernel through 5.3.2, cfg80211_mgd_wext_giwessid in net/wireless/wext-sme.c does not reject a long SSID IE, leading to a Buffer Overflow.	5.3.2	Vendor - Linux CVE Id - SBV-107962 CVSS Base - 9.8 Reporting Date - 10/04/2019 Vendor's Advisory - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-17133
vBulletin <= 5.5.4 Remote Code Execution Vulnerability - CVE-2019-17132, CVE-2019-17271	vBulletin through 5.5.4 is prone to a remote code execution vulnerability due to mishandling of custom avatars.	<=5.5.4	Vendor - vBulletin CVE Id - SBV-108109, SBV-108108 CVSS Base - 9.8 Reporting Date - 10/04/2019 Vendor's Advisory - https://forum.vbulletin.com/forum/vbulletin-announcements/vbulletin-announcements_aa/4423646-vbulletin-5-5-x-5-5-2-5-5-3-and-5-5-4-security-patch-level-2