PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
cpujan2019-5072801-Enterprise-Manager-Products-Suite] Oracle Enterprise Manager Base Platform Remote Code Execution Vulnerability in Agent Next Gen (Jython) - CVE-2016-4000	ython, as used in the Agent Next Gen component of Oracle Enterprise Manager Base Platform 12.1.0.5, 13.2.0, and 13.3.0, allows attackers to execute arbitrary code via a crafted serialized PyFunction object.	Oracle Version(s) <= 12.1.0.5, 13.3.0, 13.2.0	Published - Jan 15, 2019 CVE-2016-4000 CVSS - 9.8 Vendor's Advisory - https://nvd.nist.gov/vuln/detail/CVE-2016-4000 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4000
[MS19-JAN] Microsoft Windows DHCP Client Remote Code Execution Vulnerability - CVE-2019-0547	A memory corruption vulnerability exists in the Windows DHCP client when an attacker sends specially crafted DHCP responses to a client, aka "Windows DHCP Client Remote Code Execution Vulnerability." This affects Windows 10 1803, and Windows Server 1803	Microsoft Servers & Desktop OS Version(s) 1803 Datacnter x64, 1803 Standard x64, 1803 Pro x64, 1803 Pro x86, 1803 Home x64, 1803 home x86, 1803 Enterprise 2015, LTSB x64, 1803 Enterprise 2015LTSB x86, 1803 Education x64, 1803 Education x86, 1803 ARM64, 1803 Enterpise x86, 1803 Enterprise x64	Published - Jan 08, 2019 CVE-2019-0547 CVSS - 9.8 Vendor's Advisory - https://qualysguard.qualys.com/fo/common/vuln_info.php?allow_modify=1&id=91495 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0547
SIEMENS SIMATIC CP 1604 and CP 1616 Remote Information Disclosure or DoS Vulnerability - CVE-2018-13808	SIEMENS CP1604 versions before 2.8, and CP1616 versions before 2.8 are prone to an information disclosure and a denial-of-service vulnerabilities. A remote attacker could extract internal communication data or cause a Denial-of-Service condition via network access to port 23/tcp.	Siemens ICS Version(s): <2.8	Published - Jan 08, 2019 CVE-2018-13808 CVSS - 9.1 Vendor's Advisory -http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13808 , http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-13808
SAP Cloud Connector <2.11.3 Remote Weak Authentication Vulnerability - CVE-2019-0246	SAP Cloud Connector, before version 2.11.3, does not perform any authentication checks for functionalities that require user identity.	SAP Networking & Security Version(s) <2.11.3	Published - Jan 08, 2019 CVE-2019-0246 CVSS - 9.3 Vendor's Advisory - hhttp://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0246, https://nvd.nist.gov/vuln/detail/CVE-2019-0246
Jenkins Jira Plugin Remote CSRF and Weak Authorization Vulnerability - CVE-2018-1000412	An improper authorization vulnerability exists in Jenkins Jira Plugin 3.0.1 and earlier in JiraSite.java that allows attackers with Overall/Read access to have Jenkins connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	Jenkins Version(s):<=3.0.1	Published - Jan 09, 2019 CVE-2018-1000412 CVSS - 9.6 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1000412, https://nvd.nist.gov/vuln/detail/CVE-2018-1000412
Juniper JUNOS Remote Predictable IP ID Sequence Numbers Vulnerability - CVE-2019-0007	Juniper JUNOS 15.1, prior to 15.1 F5 on the vMX Series routers uses a predictable IP ID Sequence Number. A remote attacker could exploit this to attack the system and clients connecting through the device.	Juniper Networking & Security Version(s): 15.1 - 15.1F4	Published - Jan 09, 2019 CVE-2019-0007 CVSS - 9.3 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0007, https://nvd.nist.gov/vuln/detail/CVE-2019-00073
Google Chrome <69.0.3497.81 Remote Code Execution Vulnerability in WebAudio - CVE-2018-17457	An object lifecycle issue in Blink could lead to a use after free in WebAudio in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.	Google Internet & Mobile Version(s):<=69.0.3497.81	Published - Jan 09, 2019 CVE-2018-17457 CVSS - 8.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-17457, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-17457
Intel SGX Local Escalation of Privilege Vulnerability - CVE-2018-18098	Improper file verification in install routine for Intel(R) SGX SDK and Platform Software for Windows before 2.2.100 may allow an escalation of privilege via local access.	Intel Version(s): <2.4.100, <2.2.100	Published - Jan 10, 2019 CVE-2018-18098 CVSS - 8.4 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-18098, https://nvd.nist.gov/vuln/detail/CVE-2018-18098
[MS19-JAN] Microsoft ASP.NET Core Remote DoS Vulnerability - CVE-2019-0564	A denial of service vulnerability exists when ASP.NET Core improperly handles web requests, aka "ASP.NET Core Denial of Service Vulnerability." This affects ASP.NET Core 2.1 and 2.2 and Powershell Core 6.1 through 6.1.1 and 6.2.	Microsoft Dev Tools Version(s): 2.1.0 - 2.1.6, 2.2.0, 6.1 - 6.1.1, 6.2	Published - Jan 08, 2019 CVE-2019-0564 CVSS - 7.5 Vendor's Advisory - https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0564, http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0564, https://nvd.nist.gov/vuln/detail/CVE-2019-0564