PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
Adobe Acrobat and Reader Remote Information Disclosure Vulnerability - cve-2018-19721	Adobe Acrobat and Reader DC Continuous through 2018.011.20058, Acrobat and Reader Classic 2017 through 2017.011.30099 as well as Adobe Acrobat and Reader DC Classic 2015 through 2015.006.30448 are prone to remote information disclosure due to an out-of-bounds read vulnerability.	Version(s) <=2017.011.30099, <=2018.011.20058, <=2015.006.30448, <=2018.011.20058	Published - Dec 28, 2018 SBV-95898 CVSS - 7.5 Vendor's Advisory - https://www.rapid7.com/db/vulnerabilities/acrobat-cve-2018-19721 http://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2018-19721
VMware ESXi 6.5 Remote Unspecified Vulnerability	In VMware ESXi 6.5 encrypted vSphere vMotion might fail due to insufficient migration heap space. This vulnerability was published by Qualys.	Version(s) 6.5	Published - Dec 25, 2018 SBV-95725 CVSS - 9.8 Vendor's Advisory - https://qualysguard.qualys.com/fo/common/vuln_info.php?allow_modify=1&id=216178
Orange Livebox Remote Command Execution Vulnerability via Port 8080-CVE-2018-20377	Orange Livebox 00.96.320S devices allow remote attackers to discover Wi-Fi credentials via /get_getnetworkconf.cgi on port 8080, leading to full control if the admin password equals the Wi-Fi password or has the default admin value. This is related to Firmware 01.11.2017-11:43:44, Boot v0.70.03, Modem 5.4.1.10.1.1A, Hardware 02, and Arcadyan ARV7519RW22-A-L T VR9 1.2	Version(s) 00.96.0096.609es, 00.96.00.96.613, 00.96.217, 00.96.321s	Published - Jan 01, 2019 SBV-95885 CVSS - 9.8 Vendor's Advisory -http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20377 , https://nvd.nist.gov/vuln/detail/CVE-2018-20377
Python <3.7.1 Remote Integer Overflow Vulnerability - CVE-2018-20406	Modules/_pickle.c in Python before 3.7.1 has an integer overflow via a large LONG_BINPUT value that is mishandled during a "resize to twice the size" attempt. This issue might cause memory exhaustion, but is only relevant if the pickle format is used for serializing tens or hundreds of gigabytes of data.	Version(s) <3.7.1	Published - Dec 31, 2018 SBV-95700 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20406, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-20406, https://bugs.python.org/issue34656
Vtiger CRM 7.1.0 Remote PHP Code Execution	VTiger CRM version 7.1.0 allows attackers to upload files with a "PHP3" extension. A remote attacker can exploit this issue to execute arbitrary PHP code.	Version(s) 7.1.0	Published - Dec 27, 2018 SBV-95966 CVSS - 9.8 Vendor's Advisory - https://www.exploit-db.com/exploits/46065
JasPer 2.0.14 Remote DoS Vulnerability · CVE-2018-20622	JasPer 2.0.14 has a memory leak in base/jas_malloc.c in libjasper.a when "--output-format jp2" is used.	Version(s) 2.0.14	Published - Dec 31, 2018 SBV-95888 CVSS - 7.5 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20622, https://nvd.nist.gov/vuln/detail/CVE-2018-20622, https://github.com/mdadams/jasper/issues/193
IBM API Connect Remote Privilege Escalation Vulnerability - CVE-2018-1859	IBM API Connect 5.0.0.0 through 5.0.8.4 could allow a user authenticated as an administrator with limited rights to escalate their privileges.	Version(s) 5.0.0.0 - 5.0.8.4	Published - Jan 02, 2019 SBV-95993 CVSS - 4.3 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1859, https://nvd.nist.gov/vuln/detail/CVE-2018-1859, https://www.ibm.com/support/docview.wss?uid=ibm10792055
Xerox Altalink Remote Code Execution Vulnerability - CVE-2018-17172	The web application on Xerox AltaLink B80xx before 100.008.028.05200, C8030/C8035 before 100.001.028.05200, C8045/C8055 before 100.002.028.05200, and C8070 before 100.003.028.05200 allows unauthenticated command injection.	Version(s) <100.001.028.05200, <100.002.028.05200, <100.003.028.05200, <100.008.028.05200	Published - Jan 03, 2019 SBV-95979 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-17172, https://nvd.nist.gov/vuln/detail/CVE-2018-17172, https://securitydocs.business.xerox.com/wp-content/uploads/2018/12/cert_Security_Mini_Bulletin_XRX18AL_for_ALB80xx-C80xx_v1.1.pdf
FreeBSD Remote Code Execution or DoS Vulnerability - CVE-2018-17161	In FreeBSD before 11.2-STABLE(r348229), 11.2-RELEASE-p7, 12.0-STABLE(r342228), and 12.0-RELEASE-p1, insufficient validation of network-provided data in bootpd may make it possible for a malicious attacker to craft a bootp packet which could cause a stack buffer overflow. It is possible that the buffer overflow could lead to a Denial of Service or remote code execution.	Version(s) 11.3 -11.9, <11.2\-stable, <11.2\-RELEASE\-p7	Published - Jan 03, 2019 SBV-95971 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-17161, https://nvd.nist.gov/vuln/detail/CVE-2018-17161, https://security.freebsd.org/advisories/FreeBSD-SA-18:15.bootpd.asc
IBM i Access <=7.1 for Windows Local Code Execution Vulnerability in LoadLibrary - CVE-2018-1888	An untrusted search path vulnerability in IBM i Access for Windows versions 7.1 and earlier on Windows can allow arbitrary code execution via a Trojan horse DLL in the current working directory, related to use of the LoadLibrary function.	Version(s) <=7.1	Published - Jan 04, 2019 SBV-95994 CVSS - 4.8 Vendor's Advisory - https://www.ibm.com/support/docview.wss?uid=ibm10740233, http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1888, https://nvd.nist.gov/vuln/detail/CVE-2018-1888