PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
[APSB18-02] Adobe Acrobat and Reader Remote Code Execution Vulnerability - CVE-2018-4885	Adobe Acrobat and Reader DC Continuous through 2018.009.20050, Acrobat and Reader 2017 through 2017.011.30070 as well as Adobe Acrobat and Reader DC Classic Track through 2015.006.30394 are prone to a remote code execution vulnerability due to Out-of-bounds Read issue.	Version(s): <= 2017.011.30070	Published - February 03, 2018 CVE-2018-4885 CVSS - 8.8 Vendor's Advisory -http://www.securityfocus.com/bid/102996 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4885
Python 2.7 Heap-Buffer-Overflow and Heap-Use-After-Free Vulnerability - CVE-2018-1000030	Python 2.7.14 is vulnerable to a Heap-Buffer-Overflow as well as a Heap-Use-After-Free. Python versions prior to 2.7.14 may also be vulnerable and it appears that Python 2.7.17 and prior may also be vulnerable however this has not been confirmed. The vulnerability lies when multiply threads are handling large amounts of data. In both cases there is essentially a race condition that occurs. For the Heap-Buffer-Overflow, Thread 2 is creating the size for a buffer, but Thread1 is already writing to the buffer without knowing how much to write. So when a large amount of data is being processed, it is very easy to cause memory corruption using a Heap-Buffer-Overflow. As for the Use-After-Free, Thread3->Malloc->Thread1->Free's->Thread2-Re-uses-Free'd Memory. The PSRT has stated that this is not a security vulnerability due to the fact that the attacker must be able to run code, however in some situations, such as function as a service, this vulnerability can potentially be used by an attacker to violate a trust boundary, as such the DWF feels this issue deserves a CVE.	Version(s): <= 2.7.14	Published - February 09, 2018 CVE-2018-1000030 CVSS - 7.8 Vendor's Advisory - https://bugs.python.org/issue31530 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1000030
VMWare Virtual Appliances Information Disclosure Vulnerability via Rogue Data Cache Load (Meltdown) - CVE-2017-5754	The following VMWare virtual appliances: vCloud Usage Meter versions 3.x, Identity Manager versions 2.x and 3.x, vCenter Server Appliance versions 5.5, 6.0, 6.5, vSphere Data Protection (VDP) versions 6.x, vSphere Integrated Containers versions 1.x before 1.3, and vRealize Automation versions 6.*, 7.* are vulnerable to information disclosure in the form of memory read via bounds check bypass. A local attacker can exploit CPU data cache timing to read arbitrary locations in virtual memory, including those allocated to other virtual machines on the same host.	Version(s): <= 3.*, 2.*, 6.*, 7.*	Published - February 16, 2018 CVE-2018-5754 CVSS - 5.6 Vendor's Advisory - http://www.securityfocus.com/bid/102378 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-5754
IBM iNotes SUService and IBM Client Application Access DLL Search Order Hijacking Vulnerability - CVE-2017-1711	IBM iNotes SUService in Notes versions 9.0.1 through 9.0.1 FP10, 9.0 through 9.0 IF4, 8.5.3 through 8.5.3 FP6 IF15, 8.5.2 through 8.5.2 FP4 IF3, 8.5.1. through 8.5.1 FP5 IF3, and 8.5, and IBM Client Application Access versions 1.0.1, 1.0.1.1, and 1.0.1.1 IF1 are vulnerable to a remote code execution due to a DLL search order hijacking vulnerability. A local attacker could place malicious code in the temp directory masquerading as a windows, causing the affected product to run the malicious code.	Version(s): <= 8.5.2 - 8.5.2 FP4 IF3, 9.0 - 9.0 IF4, 8.5.3 - 8.5.3 FP6 IF15, 8.5.1. - 8.5.1 FP5 IF3, 9.0.1 - 9.0.1 FP10, 8.5	Published - February 12, 2018 CVE-2018-1711 CVSS - 5.3 Vendor's Advisory - https://www-01.ibm.com/support/docview.wss?uid=swg22010774 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-1711
Linux Kernel Remote File System Read or Write Vulnerability in NFS Server - CVE-2018-1000028	Linux kernel version after commit bdcf0a423ea1 (4.15-rc4+, 4.14.8+, 4.9.76+, 4.4.111+) contains an incorrect access control vulnerability in the NFS server (nfsd) that can result in remote users reading or writing files they should not be able to via NFS. This attack appear to be exploitable if NFS server exports a filesystem with the "rootsquash" options enabled. This vulnerability appears to have been fixed in commit 1995266727fa.	Version(s): <= 4.9.76, 4.15\-rc4, 4.4.111, 4.14.8	Published - February 09, 2018 CVE-2018-1000028 CVSS - 7.3 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1000028 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1000028
Apple MacOS X <10.13.3 Remote Code Execution Vulnerability in Touch Bar Support - CVE-2018-4083	Apple MacOS X before 10.13.3 is vulnerable to use-after-free in the kernel's IOUserClient class. AppleEmbeddedOSSupportHostClient::registerNotificationPort can be manipulated to allow access to an unreachable memory location. A remote attacker could exploit this issue to execute arbitrary code with system privileges on the affected system via a crafted application.	Version(s): < 10.13.3	Published - February 09, 2018 CVE-2018-4083 CVSS - 7.8 Vendor's Advisory - https://support.apple.com/en-il/HT208465 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-4083
PostgreSQL Remote Memory Read Vulnerability via Insert to Partitioned Table - CVE-2018-1052	PostgreSQL 10.x before 10.2 is vulnerable to memory disclosure in table partitioning, allowing an authenticated attacker to read arbitrary bytes of server memory via purpose-crafted insert to a partitioned table.	Version(s): 10 - 10.1	Published - February 09, 2018 CVE-2018-1052 CVSS - 4.3 Vendor's Advisory - https://www.postgresql.org/about/news/1829/ http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1052
[cisco-sa-20180207-rv13x] Cisco RV132W, RV134W Router Remote Code Execution Vulnerability or DoS - CVE-2018-0125	A vulnerability in the web interface of the Cisco RV132W ADSL2+ Wireless-N VPN and RV134W VDSL2 Wireless-AC VPN Routers using firmware before 1.0.1.11 could allow an unauthenticated, remote attacker to execute arbitrary code and gain full control of an affected system, including issuing commands with root privileges. The attacker could also cause an affected system to reload, resulting in a denial of service (DoS) condition. The vulnerability is due to an incomplete input validation on user-controlled input in an HTTP request to the targeted device. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected system. A successful exploit could allow the attacker to execute arbitrary code as the root user and gain full control of the affected system or cause it to reload, resulting in a DoS condition. This vulnerability is fixed in firmware version 1.0.1.11 for the following Cisco products: RV132W ADSL2+ Wireless-N VPN Router and RV134W VDSL2 Wireless-AC VPN Router. Cisco Bug IDs: CSCvg92737, CSCvh60170.	Version(s): < 1.0.1.11	Published - February 07, 2018 CVE-2018-81457 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0125 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0125