PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
Vmware Workstation and Fusion Remote Program Execution Vulnerability via Unity	VMware Workstation before 14.1.0 and Fusion before 10.1.0 contain a guest access control vulnerability. This issue may allow program execution via Unity on locked Windows VMs. VMware Tools must be updated to 10.2.0 for each VM to resolve CVE-2017-4945. VMware Tools 10.2.0 is consumed by Workstation 14.1.0 and Fusion 10.1.0 by default.	Version(s): <= 14.1.0 and Fusion <= 10.1.0	Published - January 05, 2018 CVE-2017-4945 CVSS - 9.8 Vendor's Advisory -https://www.vmware.com/security/advisories/VMSA-2018-0003.html https://nvd.nist.gov/vuln/detail/CVE-2017-4945
Western Digital MyCloud and MyCloud Mirror Contains a Backdoor	Western Digital MyCloud and My Cloud Mirror with firmware 2.30.165 and earlier on MyCloud Gen 2, PR2100, PR4100, EX2 Ultra, EX2, EX4, EX2100, EX4100, DL2100 and DL4100 contains a backdoor that allows an attacker to gain unauthorized administrative control on the affected device.	Version(s): <= 2.30.165	Published - January 04, 2018 SBV-79932 CVSS - 9.8 Vendor's Advisory - http://gulftech.org/advisories/WDMyCloud%20Multiple%20Vulnerabilities/125
Western Digital MyCloud and My Cloud Mirror <=2.30.165 Remote Code Execution Vulnerability	Western Digital MyCloud and My Cloud Mirror with firmware 2.30.165 and earlier on MyCloud Gen 2, PR2100, PR4100, EX2 Ultra, EX2, EX4, EX2100, EX4100, DL2100 and DL4100 allow a remote attacker to upload arbitrary file and execute arbitrary code via a crafted post request.	Version(s): <=2.30.165	Published - January 04, 2018 SBV-79933 CVSS - 9.8 Vendor's Advisory - http://gulftech.org/advisories/WDMyCloud%20Multiple%20Vulnerabilities/125
Western Digital MyCloud and My Cloud Mirror <=2.30.165 Remote Multiple Vulnerabilities	Western Digital MyCloud and My Cloud Mirror with firmware 2.30.165 and earlier on MyCloud Gen 2, PR2100, PR4100, EX2 Ultra, EX2, EX4, EX2100, EX4100, DL2100 and DL4100 is prone to multiple vulnerabilities including denial of service, command injection and information disclosure.	Version(s): <= 2.30.165	Published - January 04, 2018 SBV-79931 CVSS - 9.8 Vendor's Advisory - http://gulftech.org/advisories/WDMyCloud%20Multiple%20Vulnerabilities/125
ImageInject Plugin for WordPress CSRF Vulnerability	The ImageInject plugin 1.15 for WordPress has CSRF via wp-admin/options-general.php.	Version(s): 1.15	Published - January 08, 2018 CVE-2018-5285 CVSS - 9.6 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5285 https://nvd.nist.gov/vuln/detail/CVE-2018-5285
Gravity Upload Ajax Plugin for WordPress Remote Code Execution Vulnerability	Unrestricted file upload vulnerability in the Gravity Upload Ajax plugin 1.1 and earlier for WordPress allows remote attackers to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file under wp-content/uploads/gravity_forms.	Version(s): <= 1.1	Published - January 08, 2018 CVE-2014-4972 CVSS - 9.8 Vendor's Advisory - https://wpvulndb.com/vulnerabilities/8232 https://nvd.nist.gov/vuln/detail/CVE-2014-4972
Linux Kernel <4.13.6 Use-After-Free flaw in fs/userfaultfd.c	A use-after-free flaw was found in fs/userfaultfd.c in the Linux kernel before 4.13.6. The issue is related to the handling of fork failure when dealing with event messages. Failure to fork correctly can lead to a situation where a fork event will be removed from an already freed list of events with userfaultfd_ctx_put().	Version(s): < 4.13.6	Published - January 14, 2018 CVE-2017-15126 CVSS - 9.8 Vendor's Advisory - https://access.redhat.com/security/cve/CVE-2017-15126 https://bugzilla.redhat.com/show_bug.cgi?id=1523481 https://nvd.nist.gov/vuln/detail/CVE-2017-15126