PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
Mozilla Firefox for Android <51.0.3 Remote Unspecified Vulnerability	Mozilla Firefox for Android before 51.0.3 is prone to an unspecified vulnerability due to improper configuration of the cache directory, updated as world writable.	Version(s): Mozilla Firefox before 51.0.3	Published - February 09, 2017 CVE-2017-5397 CVSS - 9.3 Vendor's Advisory Available at : https://www.mozilla.org/en-US/firefox/android/
Adobe Flash Player <=24.0.0.194 Remote Code Execution due to a Use-After-Free Issue - CVE-2017-2985	Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable use after free vulnerability in the ActionScript 3 BitmapData class. Successful exploitation could lead to arbitrary code execution.	Version(s): Adobe Flash Player versions 24.0.0.194 and earlier.	Published - February 14, 2017 CVE-2017-2985 CVSS - 9.3 Vendor's Advisory Available at: https://helpx.adobe.com/security/products/flash-player/apsb17-04.html
Adobe Flash Player <=24.0.0.194 Remote Code Execution due to an Integer-Overflow Issue - CVE-2017-2987	Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable integer overflow vulnerability related to Flash Broker COM. Successful exploitation could lead to arbitrary code execution.	Version(s): Adobe Flash Player versions 24.0.0.194	Published - February 14, 2017 CVE-2017-2987 CVSS - 9.3 Vendor's Advisory Available at : Https://helpx.adobe.com/security/products/flash-player/apsb17-04.html
Microsoft Security Update for Adobe Flash Player Heap-Buffer-Overflow Issue - CVE-2017-2984	Adobe Flash Player versions 24.0.0.194 and earlier, running on Windows 8.1, Windows Server 2012, Server 2012 R2, Windows 10 and Windows Server 2016, have an exploitable heap overflow vulnerability in the h264 decoder routine. Successful exploitation could lead to arbitrary code execution.	Version(s): Adobe Flash Player versions 24.0.0.194 and earlier.	Published - February 14, 2017 CVE-2017-2984 CVSS - 9.3 Vendor's Advisory Available at: https://portal.msrc.microsoft.com/en-us/eula
Microsoft Security Update for Adobe Flash Player Memory-Corruption Issue - CVE-2017-2991	Adobe Flash Player versions 24.0.0.194 and earlier, running on Windows 8.1, Windows Server 2012, Server 2012 R2, Windows 10 and Windows Server 2016, have an exploitable memory corruption vulnerability in the h264 codec (related to decompression). Successful exploitation could lead to arbitrary code execution.	Version(s): Adobe Flash Player versions 24.0.0.194 and earlier.	Published - February 14, 2017 CVE-2017-2991 CVSS - 9.3 Vendor's Advisory Available at : https://helpx.adobe.com/security/products/flash-player/apsb17-04.html
Adobe Flash Player <=24.0.0.194 Remote Code Execution due to a Memory-Corruption Issue - CVE-2017-2996	Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable memory corruption vulnerability in Primetime SDK. Successful exploitation could lead to arbitrary code execution.	Version(s):Adobe Flash Player versions 24.0.0.194 and earlier.	Published - February 14, 2017 CVE-2017-3792 CVSS - 10.0 Vendor's Advisory Available at: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170125-telepresence
Microsoft Security Update for Adobe Flash Player Use-After-Free Issue - CVE-2017-2982	Adobe Flash Player versions 24.0.0.194 and earlier, running on Windows 8.1, Windows Server 2012, Server 2012 R2, Windows 10 and Windows Server 2016, have an exploitable use after free vulnerability in a routine related to player shutdown. Successful exploitation could lead to arbitrary code execution.	Version(s): Adobe Flash Player versions 24.0.0.194 and earlier.	Published - February 21, 2017 CVE-2017-2982 CVSS - 9.3 Vendor's Advisory Available at : https://helpx.adobe.com/security/products/flash-player/apsb17-04.html
Oracle Java Remote MITM, XXE Attacks due to Improper Handling of Usernames in FTP URL	Oracle Java allows a remote attacker to bypass firewall restrictions and inject commands via TCP connections .This issue exists due to improper handling of carriage returns and line feeds in usernames in the FTP URL (sun.net.ftp.impl.FtpClient). The flaw may be leveraged to carry out man-in-the-middle attacks, server-side request forgery, XML external Entity attacks or to send unauthorized email from Java applications. This vulnerability was published by SecurityFocus.	Version(s):Oracle JDK and JRE all versions.	Published - February 21, 2017 SBV-68859 CVSS - 10.0 Vendor's Advisory Available at: http://www.theregister.co.uk/2017/02/21/java_python_ftp_code_vulnerable/
Microsoft Security Update for Adobe Flash Player Heap-Buffer-Overflow Issue - CVE-2017-2986	Adobe Flash Player versions 24.0.0.194 and earlier, running on Windows 8.1, Windows Server 2012, Server 2012 R2, Windows 10 and Windows Server 2016, have an exploitable heap overflow vulnerability in the Flash Video (FLV) codec. Successful exploitation could lead to arbitrary code execution.	Version(s): Adobe Flash Player versions 24.0.0.194 and earlier	Published - February 14, 2017 CVE-2017-2986 CVSS - 9.3 Vendor's Advisory Available at : https://portal.msrc.microsoft.com/en-us/eula
Microsoft Security Update for Adobe Flash Player Heap-Buffer-Overflow Issue - CVE-2017-2992	Adobe Flash Player versions 24.0.0.194 and earlier, running on Windows 8.1, Windows Server 2012, Server 2012 R2, Windows 10 and Windows Server 2016, have an exploitable heap overflow vulnerability when parsing an MP4 header. Successful exploitation could lead to arbitrary code execution.	Version(s): Adobe Flash Player versions 24.0.0.194 and earlier.	Published - February 14, 2017 CVE-2017-2992 CVSS - 9.3 Vendor's Advisory Available at: https://helpx.adobe.com/security/products/flash-player/apsb17-04.html