PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
Win32/WannaCrypt attack using an exploit code for a patched SMB vulnerability, CVE-2017-0145	Samples show the WannaCry malware with no AV detection. There is a Visual Basic Script file (VBS) packaged with some binaries hinting at possible initial infection vectors via emails with linked or attached Microsoft Office documents. Once installed, it encrypts files using AES and RSA encryption, locks them by encrypting data and then extorts money to let users back in.	Version(s):unpatched Windows 7 and Windows Server 2008 (or earlier OS) systems	Published - May 12, 2017 CVE-2017-0145 CVSS - 9.3 Vendor's Advisory - https://www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?Name=Ransom:Win32/WannaCrypt https://blogs.technet.microsoft.com/mmpc/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/
Adobe Flash Player Remote Code Execution Vulnerability due to Use-After-Free	Adobe Flash Player version 25.0.0.148 and earlier (on MacOS version 25.0.0.163 and earlier) is prone to remote code execution due to a use after free vulnerability when masking display objects.	Version(s): Adobe Flash Player version 25.0.0.148 and earlier (on MacOS version 25.0.0.163 and earlier)	Published - May 09, 2017 CVE-2017-3071 CVSS - 9.3 Vendor's Advisory - http://www.securityfocus.com/bid/98347
Microsoft Office Remote Code Execution Vulnerability	Microsoft Office 2016, 2010 SP2 and 2013 SP1 allow remote attackers to execute arbitrary code via a crafted EPS file. Successful attacks of this vulnerability can result in gaining control of the affected system.	Version(s): Microsoft Office 2016, 2010 SP2 and 2013 SP1	Published - May 09, 2017 CVE-2017-0262 CVSS - 9.3 Vendor's Advisory - http://www.securityfocus.com/bid/98279
Microsoft Windows COM Elevation of Privilege Vulnerability	Microsoft Windows 7, Windows 8.1 and Windows 10, Windows 10 1607, Windows 10 1511 and Windows 10 1703, Windows Server 2008, 2008 R2, 2012, 2012 R2 and Server 2016 are prone to a privilege escalation vulnerability due to a COM Aggregate Marshaler component. An attacker can exploit this vulnerability by using a specially crafted application.	Version(s): Microsoft Windows 7, Windows 8.1 and Windows 10, Windows 10 1607, Windows 10 1511 and Windows 10 1703, Windows Server 2008, 2008 R2, 2012, 2012 R2 and Server 2016	Published - May 09, 2017 CVE-2017-0213 CVSS - 9.3 Vendor's Advisory - http://www.securityfocus.com/bid/98102
Microsoft Windows Remote Code Execution in Adobe Flash Player	Memory corruption in Adobe Flash Player 25.0.0.148 and earlier on Microsoft Windows 8.1, Server 2012, Server 2012 R2, Windows 10, and Server 2016 allows a remote attacker to execute arbitrary code due to a flaw in the BlendMode class.	Version(s):Microsoft Windows 8.1, Server 2012, Server 2012 R2, Windows 10, and Server 2016	Published - May 09, 2017 CVE-2017-3069 CVSS - 9.3 Vendor's Advisory -https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV170006
Linux Kernel <=4.10.15 net/ipv4/inet_connection_sock.c Remote DoS or Other Unspecified Vulnerability	The inet_csk_clone_lock function in net/ipv4/inet_connection_sock.c in the Linux kernel through 4.10.15 allows attackers to cause a denial of service (double free) or possibly have unspecified other impact by leveraging use of the accept system call.	Version(s):Linux kernel through 4.10.15	Published - May 10, 2017 CVE-2017-8890 CVSS - 10.0 Vendor's Advisory - http://www.securityfocus.com/bid/98562
Apple MacOS X <10.12.5 Remote Code Execution Vulnerability in CoreFoundation	Apple MacOS X before 10.12.5 is prone to a remote code execution vulnerability in CoreFoundation due to a memory corruption issue. A remote attacker could exploit this issue to execute arbitrary code on the affected system.	Version(s): Apple MacOS X before 10.12.5	Published - May 15, 2017 CVE-2017-2522 CVSS - 9.3 Vendor's Advisory - http://www.securityfocus.com/bid/98588
Microsoft Microsoft PowerPoint for Mac Remote Code Execution Vulnerability	Memory corruption in Microsoft PowerPoint for Mac 2011 allows a remote attacker to execute arbitrary code via a crafted file.	Version(s): Microsoft PowerPoint for Mac 2011	Published - May 02, 2017 CVE-2017-0265 CVSS - 9.3 Vendor's Advisory - http://www.securityfocus.com/bid/98285
Microsoft Windows Remote Code Execution in Adobe Flash Player	Memory corruption in Adobe Flash Player 25.0.0.148 and earlier on Microsoft Windows 8.1, Server 2012, Server 2012 R2, Windows 10, and Server 2016 allows a remote attacker to execute arbitrary code due to a flaw in the Advanced Video Coding engine.	Version(s): Microsoft Windows 8.1, Server 2012, Server 2012 R2, Windows 10, and Server 2016	Published - May 09, 2017 CVE-2017-3068 CVSS - 10.0 Vendor's Advisory - https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV170006