PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
Microsoft Office Memory Corruption Vulnerability	Microsoft Word 2016 and SharePoint Enterprise Server 2016 allow remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office Memory Corruption Vulnerability."	Version(s): Microsoft Word 2016 and SharePoint Enterprise Server 2016	Published - January 10, 2017 CVE-2017-0003 CVSS - 9.3 Vendor's Advisory Available at : https://technet.microsoft.com/library/security/ms17-002
Adobe Flash Player <=24.0.0.186 Remote Memory-Corruption Vulnerability	Adobe Flash Player versions 24.0.0.186 and earlier have an exploitable memory corruption vulnerability related to setting visual mode effects. Successful exploitation could lead to arbitrary code execution.	Version(s): Adobe Flash Player versions 24.0.0.186 and earlier	Published - January 10, 2017 CVE-2017-2928 CVSS - 9.3 Vendor's Advisory Available at: http://www.securityfocus.com/bid/95350
Adobe Acrobat DC, Reader DC, Acrobat XI and Reader XI Code Execution Vulnerability	Adobe Acrobat Reader versions 15.020.20042 and earlier, 15.006.30244 and earlier, 11.0.18 and earlier have an exploitable memory corruption vulnerability in the image conversion module when handling malformed TIFF images. Successful exploitation could lead to arbitrary code execution.	Version(s): Adobe Acrobat Reader versions 15.020.20042 and earlier, 15.006.30244 and earlier, 11.0.18 and earlier	Published - January 10, 2017 CVE-2017-2954 CVSS - 9.3 Vendor's Advisory Available at: https://helpx.adobe.com/security/products/acrobat/apsb17-01.html
Microsoft Windows Remote Code Execution in Adobe Flash Player	Adobe Flash Player versions 24.0.0.186 on Microsoft Windows 8.1, Windows Server 2012, Windows Server 2012 R2, Windows 10, and Windows Server 2016 and earlier have an exploitable heap overflow vulnerability when processing Adobe Texture Format files. Successful exploitation could lead to arbitrary code execution.	Version(s): Adobe Flash Player versions 24.0.0.186 and earlier	Published - January 10, 2017 CVE-2017-2927 CVSS - 9.3 The vendor's advisory is available at: https://technet.microsoft.com/library/security/ms17-003
Google Android <=7.1 Remote Code Execution in Qualcomm Bootloader	Qualcomm bootloader in Google Android 7.1 and earlier before 2017-01-05 on Nexus 6P, Pixel and Pixel XL allows remote attackers to execute arbitrary code via a crafted application, aka Android internal bug 31399736.	Version(s): Google Android 7.1 and earlier before 2017-01-05 on Nexus 6P, Pixel and Pixel XL	Published -January 03,2017 CVE-2016-8423 CVSS - 9.3 Vendor's Advisory Available at https://source.android.com/security/bulletin/2017-01-01.html
Google Android 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0 and 7.1 Remote Code Execution in Mediaserver	Mediaserver in Google Android 5.0 through 5.0.2, 5.1.0 through 5.1.1, 6.0, 6.0.1, 7.0 and 7.1 before 2017-01-01 allows remote attackers to execute arbitrary code via a crafted file, aka Android internal bug 31607432.	Version(s): Google Android 5.0 through 5.0.2, 5.1.0 through 5.1.1, 6.0, 6.0.1, 7.0 and 7.1 before 2017-01-01	Published -January 03, 2017 CVE-2016-0381 CVSS - 9.3 The vendor's advisory is available at: https://source.android.com/security/bulletin/2017-01-01.html
Google Android <=7.1 on Nexus 9 Remote Privilege Escalation in NVIDIA GPU Driver	NVIDIA GPU driver in Google Android 7.1 and earlier before 2017-01-05 on Nexus 9, allows remote attackers to execute arbitrary code with kernel privileges via a crafted application, aka Android internal bug 31799863.	Version(s): Google Android 7.1 and earlier before 2017-01-05 on Nexus 9	Published -January 03,2017 CVE-2016-8482 CVSS - 9.3 Vendor's Advisory Available at http://source.android.com/security/bulletin/2017-01-01.html
Google Android <=7.1 Remote Code Execution due to a Flaw in MediaTek Components	MediaTek components in Google Android 7.1 and earlier before 2017-01-05 allows remote attackers to execute arbitrary code via a crafted application, aka Android internal bug 31749463.	Version(s): Google Android 7.1 and earlier before 2017-01-05	Published -January 03, 2017 CVE-2016-8447 CVSS - 9.3 The vendor's advisory is available at: https://source.android.com/security/bulletin/2017-01-01.html
Google Android <=7.1 Remote Code Execution due to a Flaw in Qualcomm Wi-Fi Driver	Qualcomm Wi-Fi driver in Google Android 7.1 and earlier before 2017-01-05 on Nexus 5X, Android One, Pixel and Pixel XL allows remote attackers to execute arbitrary code via a crafted application, aka Android internal bug 32506396.	Version(s): Google Android 7.1 and earlier before 2017-01-05 on Nexus 5X, Android One, Pixel and Pixel XL	Published -January 03,2017 CVE-2016-8452 CVSS - 9.3 Vendor's Advisory Available at https://source.android.com/security/bulletin/2017-01-01.html
Google Android <=7.1 Remote Code Execution due to a Flaw in the Kernel Profiling Subsystem	The kernel profiling subsystem in Google Android 7.1 and earlier before 2017-01-05 on Nexus 5X, Nexus 6, Nexus 6P, Nexus 9, Android One, Pixel C and Nexus Player allows remote attackers to execute arbitrary code via a crafted application, aka Android internal bug 32659848.	Version(s):Google Android 7.1 and earlier before 2017-01-05 on Nexus 5X, Nexus 6, Nexus 6P, Nexus 9, Android One, Pixel C and Nexus Player	Published -January 03, 2017 CVE-2016-9754 CVSS - 9.3 The vendor's advisory is available at: https://source.android.com/security/bulletin/2017-01-01.html
Cisco CloudCenter Orchestrator Docker Engine <4.6.2 Remote Escalation of Privileges Vulnerability	Cisco CloudCenter Orchestrator before 4.6.2 is prone to an elevation of privileges due to misconfiguration that could allow a remote unauthenticated attacker to reach the docker engine ports from outside the CloudCenter Orchestrator system. The attacker can exploit this vulnerability to load docker containers on the affected system with higher privileges.	Version(s): Cisco CloudCenter Orchestrator before 4.6.2	Published -December 21, 2016 CVE-2016-9223 CVSS - 9.3 Vendor's Advisory Available at https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161221-cco
Google Android 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1 Remote Elevation of Privileges in Libnl	Libnl in Google Android 5.0 through 5.0.2, 5.1.0 through 5.1.1, 6.0, 6.0.1, 7.0 and 7.1 before 2017-01-01, allows remote attackers to execute arbitrary code with higher permissions via a malicious application. The application would have could execute code within the context of a privileged process Aka Android internal bug 32255299.	Version(s):Google Android 5.0 through 5.0.2, 5.1.0 through 5.1.1, 6.0, 6.0.1, 7.0 and 7.1 before 2017-01-01	Published -January 01, 2017 CVE-2017-0386 CVSS - 9.3 The vendor's advisory is available at: http://source.android.com/security/bulletin/2017-01-01.html
Google Android 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1 Remote Elevation of Privileges in Audioserver	Audioserver in Google Android 4.0 through 4.4.4, 5.0 through 5.0.2, 5.1.0 through 5.1.1, 6.0, 6.0.1, 7.0 and 7.1 before 2017-01-01, allows remote attackers to execute arbitrary code with higher permissions via a malicious application. The application would have could execute code within the context of a privileged process Aka Android internal bug 32585400.	Version(s): Google Android 4.0 through 4.4.4, 5.0 through 5.0.2, 5.1.0 through 5.1.1, 6.0, 6.0.1, 7.0 and 7.1 before 2017-01-01	Published -January 01, 2017 CVE-2017-0385 CVSS - 9.3 Vendor's Advisory Available at http://source.android.com/security/bulletin/2017-01-01.html
Google Android <=7.1 Remote Code Execution due to a Flaw in Qualcomm Camera	Qualcomm camera in Google Android 7.1 and earlier before 2017-01-05 on Nexus 5X, Nexus 6, Nexus 6P, Android One, Pixel and Pixel XL allows remote attackers to execute arbitrary code via a crafted application, aka Android internal bug 31225246.	Version(s): Google Android 7.1 and earlier before 2017-01-05 on Nexus 5X, Nexus 6, Nexus 6P, Android One, Pixel and Pixel XL	Published -January 03, 2017 CVE-2016-8412 CVSS - 9.3 The vendor's advisory is available at: https://source.android.com/security/bulletin/2017-01-01.html