PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
Microsoft Malware Protection Engine Remote Code Execution Vulnerability-CVE-2017-0290	Microsoft Malware Protection Engine version 1.1.13701.0 and earlier, as used in multiple Microsoft antimalware products, is prone to a critical remote code execution vulnerability due to a memory corruption issue. A remote attacker could exploit this issue via a specially crafted file that would be scanned by the Malware Protection Engine. Successful exploitation would allow the attacker to execute arbitrary code with LocalSystem privileges and take full control of the system. Microsoft has released a fix for this issue in the automatically updated malware definitions for the affected products. The products vulnerable to this issue are: Forefront Endpoint Protection 2010; Microsoft Endpoint Protection; Forefront Security for SharePoint Service Pack 3; System Center Endpoint Protection; Security Essentials; Windows Defender for Windows 7; Windows Defender for Windows 8.1; Windows Defender for Windows RT 8.1; Windows Defender for Windows 10, Windows 10 1511, Windows 10 1607, Windows Server 2016, and Windows 10 1703; Windows Intune Endpoint Protection.	Version(s): <=1.1.13701.0	Published - May 06, 2017 CVE-2017-0290 CVSS - 9.3 Vendor's Advisory - https://technet.microsoft.com/en-us/library/security/4022344.aspx
Google Android <=7.1.2 Remote DoS or Privilege Escalation Vulnerability	Linux kernel before 3.19 as used in Google Android version 7.1.2 and earlier before 2017-05-05 in Nexus 6, 9, Pixel C, Android One and Nexus Player allows local users to gain privileges or cause a denial of service (use-after-free) via a crafted application.	Version(s): <=7.1.2	Published - May 02, 2017 CVE-2014-9940 CVSS - 9.3 Vendor's Advisory - https://source.android.com/security/bulletin/2017-05-01
Google Android <=7.1.2 Remote Unspecified Vulnerability in Qualcomm Components	Qualcomm Components as used in Google Android 7.1.2 and earlier before 2017-05-05 on Pixel and Pixel XL allow a remote attacker to have an unspecified impact, aka Android internal bug 31624008.	Version(s): <=7.1.2	Published - May 01, 2017 CVE-2016-10278 CVSS - 9.3 Vendor's Advisory - https://source.android.com/security/bulletin/2017-05-01
Intel Active Management Technology (AMT) and Standard Manageability (ISM) Remote Privilege Escalation	Intel Active Management Technology (AMT), Standard Manageability (ISM) firmware versions 6.0 through 6.2.61.3534, 7.0 through 7.1.91.3271, 8.0 through 8.1.71.3607, 9.0 through 9.1.41.6023, 9.5 through 9.5.61.3011, 10.0 through 10.0.55.2999, 11.0 through 11.0.25.3000, and 11.5 through 11.6.27.3263 are prone to a remote privilege escalation vulnerability. A remote attacker could gain system privileges to provisioned Intel manageability SKUs.	Version(s):6.0 - 6.2.61.3534, 7.0 - 7.1.91.3271, 8.0 - 8.1.71.3607, 9.0 - 9.1.41.6023, 9.5 - 9.5.61.3011, 10.0 - 10.0.55.2999, 11.0 - 11.0.25.3000, 11.5 - 11.6.27.3263	Published - May 01, 2017 CVE-2017-5689 CVSS - 10.0 Vendor's Advisory - https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00075&languageid=en-fr
Google Android Remote Code Execution in Mediaserver	Mediaserver in Google Android 4.4 through 4.4.4, 5.0 through 5.0.2, 5.1 through 5.1.1, 6.0, 6.0.1, 7.0 and 7.1 through 7.1.1 before 2017-05-01 could allow remote attackers to execute arbitrary code via a crafted application. AKA Android internal bug 34749392.	Version(s):4.4 - 4.4.4, 5.0 - 5.0.2, 5.1 - 5.1.1, 6.0 - 6.0.1, 7.0, 7.1 - 7.1.1	Published - May 01, 2017 CVE-2017-0596 CVSS - 9.3 Vendor's Advisory - https://android.googlesource.com/platform/frameworks/av/+/5443b57cc54f2e46b35246637be26a69e9f493e1
Google Android <=7.1.2 Remote Unspecified Vulnerability in Qualcomm Components	Qualcomm Components as used in Google Android 7.1.2 and earlier before 2017-05-05 on Pixel and Pixel XL allow a remote attacker to have an unspecified impact, aka Android internal bug 31624421.	Version(s): <=7.1.2	Published - May 01, 2017 CVE-2016-10279 CVSS - 9.3 Vendor's Advisory - https://source.android.com/security/bulletin/2017-05-01
Wireless IP Camera (P2P) WIFICAM Remote Unspecified Vulnerability	Wireless IP Camera (P2P) WIFICAM devices have a backdoor root account that can be accessed with TELNET.	Version(s): Any	Published - May 02, 2017 CVE-2014-9940 CVSS - 9.3 Vendor's Advisory - https://nvd.nist.gov/vuln/detail/CVE-2017-8224
Google Android 7.1.2 on Nexus 9 Remote Privilege Escalation in NVIDIA Video Driver	Google Android 7.1.2 and earlier, before 2017-05-05, when running on Nexus 9, is prone to a critical elevation of privilege vulnerability in the NVIDIA video driver. A remote attacker could exploit this issue to execute arbitrary code with kernel privileges, if she could entice the victim to install a maliciously crafted application. AKA Android internal bug 34113000.	Version(s): <=7.1.2	Published - May 01, 2017 CVE-2017-0331 CVSS - 9.3 Vendor's Advisory - https://source.android.com/security/bulletin/2017-05-01
Google Android Remote Security Bypass in Framework APIs	Framework APIs in Google Android 6.0 through 6.0.1, 7.0 and 7.1 through 7.1.2 before 2017-05-01 could allow remote attackers to bypass restrictions via a crafted application. AKA Android internal bug 34114230.	Version(s): 4.4 - 4.4.4, 5.0 - 5.0.2, 5.1 - 5.1.1, 6.0 - 6.0.1, 7.0, 7.1 - 7.1.2	Published - May 01, 2017 CVE-2017-0593 CVSS - 9.3 Vendor's Advisory - https://source.android.com/security/bulletin/2017-05-01