PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
Google Android 7.1.2 and Earlier Unspecified Vulnerability in Qualcomm Secure Systems Group Component - CVE-2016-5871	Google Android 7.1.2 and earlier, before 2017-07-05, is prone to a high severity unspecified vulnerability in the Qualcomm secure systems group component. AKA Android internal bug 37473055.	Version(s): <=7.1.2	Published - July 05, 2017 CVE-2016-5871 CVSS - 9.3 Vendor's Advisory - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-5871 https://source.android.com/security/bulletin/2017-07-01
Google Android <=7.1.2 Remote Code Execution in the Qualcomm Video Driver - CVE-2017-8265	Google Android version 7.1.2 and earlier before 2017-07-05 is prone to a remote code execution vulnerability in the Qualcomm video driver. The flaw could enable a crafted application to execute arbitrary code within the context of the kernel. AKA Android internal bug 32341313.	Version(s): <=7.1.2	Published - July 05, 2017 CVE-2017-8265 CVSS - 9.3 Vendor's Advisory - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8265 https://source.android.com/security/bulletin/2017-07-01
Google Android <=7.1.2 Remote Elevation of Privileges in HTC Components - CVE-2017-0707	Google Android versions 7.1.2 and earlier before 2017-07-05 are prone to a remote elevation of privileges vulnerability due a flaw in HTC LED Driver. A remote attacker can exploit this issue to gain higher privileges and execute arbitrary code on the affected system using a malicious local application. Android Bug ID 36088467.	Version(s): <=7.1.2.	Published - July 05, 2017 CVE-2017-0707 CVSS - 9.3 Vendor's Advisory - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0707 https://source.android.com/security/bulletin/2017-07-01
Google Android <=7.1.2 Remote Elevation of Privileges in Broadcom Components - CVE-2017-0706	Google Android versions 7.1.2 and earlier before 2017-07-05 are prone to a remote elevation of privileges vulnerability due a flaw in Broadcom Wi-Fi Driver. A remote attacker can exploit this issue to gain higher privileges and execute arbitrary code on the affected system. Android Bug ID 35195787.	Version(s): <7.1.2	Published - July 05,2017 CVE-2017-0706 CVSS - 9.3 Vendor's Advisory - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0706 https://source.android.com/security/bulletin/2017-07-01
Google Android Remote Elevation of Privileges in Framework - CVE-2017-0664	Google Android versions 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, and 7.1.2 before 2017-07-01 are prone to a remote elevation of privileges vulnerability due a flaw in the Framework. A remote attacker can exploit this issue to execute arbitrary code on the affected system using a crafted file. Android Bug ID 36491278.	Version(s): <=5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2	Published - July 05, 2017 CVE-2017-0664 CVSS - 9.3 Vendor's Advisory - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0664 https://source.android.com/security/bulletin/2017-07-01
Google Android Remote Elevation of Privileges in System UI - CVE-2017-0703	Google Android versions 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, and 7.1.2 before 2017-07-01 are prone to a remote elevation of privileges vulnerability due a flaw in the System UI. A remote attacker can exploit this issue to execute arbitrary code on the affected system using a crafted file. Android Bug ID 33123882.	Version(s): <= 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2	Published - July 05, 2017 CVE-2017-0703 CVSS - 9.3 Vendor's Advisory - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0703 https://source.android.com/security/bulletin/2017-07-01
Google Android 4.4.4 Remote Code Execution via a Crafted File - CVE-2017-0671	Libraries in Google Android 4.4.4 before 2017-07-01 allows a remote attacker to execute arbitrary code via a crafted file. Android Bug ID 34514762.	Version(s): <= 4.4.4	Published - July 05, 2017 CVE-CVE-2017-0671 CVSS - 9.3 Vendor's Advisory - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0671 https://source.android.com/security/bulletin/2017-07-01
Google Android Remote Privilege Escalation Vulnerability in the Kernel (Networking Subsystem) - CVE-2017-6074	The dccp_rcv_state_process function in net/dccp/input.c in the Linux kernel, as used in Google Android 7.1.2 and earlier before 2017-07-05, mishandles DCCP_PKT_REQUEST packet data structures in the LISTEN state, which allows local applications to execute arbitrary code within the context of a privileged process. Android Bug ID 35784697.	Version(s): <= 7.1.2	Published - July 05, 2017 CVE-2017-6074 CVSS - 9.3 Vendor's Advisory - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-6074 https://source.android.com/security/bulletin/2017-07-01