Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India

CERT-In Advisory CIAD-2016-0073

Multiple Vulnerabilities in Google Android OS

Original Issue Date: December 08, 2016

Severity Rating: High

Systems Affected

- Google Android OS prior to 7.0

Overview

Multiple vulnerabilities have been reported in Google Android OS which could be exploited by a remote attacker to execute arbitrary code on the affected system, gain elevated privileges, obtain sensitive information or cause denial of service (DoS) condition.

Description

1. Remote Code Execution Vulnerabilities (CVE-2016-5419 CVE-2016-5420 CVE-2016-5421)

These vulnerabilities exists in CURL/LIBCURL libraries. A remote attacker could exploit these vulnerabilities using forged certificate to execute arbitrary code on the affected system.

2. Remote Code Execution Vulnerabilities (CVE-2016-6768)

This vulnerability exists in Frame sequence library. A remote attacker could exploit this vulnerability using specially crafted file to execute arbitrary code on the affected system.

3. Elevation of privilege vulnerabilities (CVE-2016-6762 CVE-2016-6769 CVE-2016-6770 CVE-2016-6771 CVE-2016-6772 CVE-2016-4794 CVE-2016-5195 CVE-2016-6775 CVE-2016-6776 CVE-2016-6777 CVE-2015-8966 CVE-2016-6915 CVE-2016-6916 CVE-2016-6917 CVE-2016-9120 CVE-2014-4014 CVE-2015-8967 CVE-2016-6778 CVE-2016-6779 CVE-2016-6780 CVE-2016-6492 CVE-2016-6781 CVE-2016-6782 CVE-2016-6783 CVE-2016-6784 CVE-2016-6785 CVE-2016-6761)

These vulnerabilities exists in "libziparchive", " Smart Lock"," Framework APIs", " Telephony", " Wi-Fi"," kernel memory subsystem", " NVIDIA GPU driver"," kernel", " NVIDIA video driver", "kernel ION driver", " kernel file system", ," HTC sound codec driver", " MediaTek driver", "Qualcomm media codecs"," Qualcomm camera driver"," kernel performance subsystem"," MediaTek I2C driver", " NVIDIA libomx library"," Qualcomm sound driver"," kernel security subsystem"," Synaptics touch screen driver", "Broadcom Wi-Fi driver" and kernel networking subsystem.
Successful exploitation of these vulnerabilities could allow an attacker to bypass security restrictions ,execute arbitrary code on the affected system and gain elevated privileges.

4. Information Disclosure Vulnerabilities (CVE-2016-6773 CVE-2016-6774 CVE-2016-8396 CVE-2016-8397 CVE-2016-6756 CVE-2016-6757 CVE-2016-8400 CVE-2016-8401 CVE-2016-8402 CVE-2016-8403)

These vulnerabilities exists in "Mediaserver", "Package Manager"," MediaTek video driver", "NVIDIA video driver", "Qualcomm components", "NVIDIA librm library", "kernel components", "NVIDIA video driver" and Qualcomm sound driver.
Successful exploitation of these vulnerabilities could allow an attacker to obtain sensitive information.

5. Denial of Service Vulnerabilities (CVE-2016-6763 CVE-2016-6766 CVE-2016-6765 CVE-2016-6764 CVE-2016-6767 CVE-2016-5341 CVE-2016-8395)

These vulnerabilities exists in "Telephony", "Mediaserver", " Qualcomm GPS component" and NVIDIA camera driver .Successful exploitation of these vulnerabilities could allow an attacker to cause Denial of Service (DoS) condition on the affected system.

Solution

Users may obtain over-the-air-updates from appropriate vendors

Vendor Information

Android
https://source.android.com/security/bulletin/2016-12-01.html

References

Android
https://source.android.com/security/bulletin/2016-12-01.html

CVE Name

CVE-2016-5419
CVE-2016-5420
CVE-2016-5421
CVE-2016-6768
CVE-2016-6760
CVE-2016-6759
CVE-2016-6758
CVE-2016-6755
CVE-2016-6786
CVE-2016-6787
CVE-2016-6788
CVE-2016-6789
CVE-2016-6790
CVE-2016-6791
CVE-2016-8391
CVE-2016-8392
CVE-2015-7872
CVE-2016-8393
CVE-2016-8394
CVE-2014-9909
CVE-2014-9910
CVE-2016-8399
CVE-2016-8404
CVE-2016-8405
CVE-2016-8406
CVE-2016-8407
CVE-2016-8408
CVE-2016-8409
CVE-2016-8410
CVE-2016-6763
CVE-2016-6766
CVE-2016-6765
CVE-2016-6764
CVE-2016-6767
CVE-2016-5341
CVE-2016-8395

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.

Contact Information

Email: info@cert-in.org.in
Phone: +91-11-24368572

Postal address

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,
New Delhi - 110 003
India