Google Android up Mediaserver buffer overflow

General Details

Affected Version	4.4, 5.1
Date of Publish	03-11-15
Varutra Vuln ID	KVA100
References	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8073
CVE ID	CVE-2015-8073
CVSSv2 Score	10

Vulnerability Summary

Vulnerability	Google Android up Mediaserver buffer overflow
Description	It was reported that the mediaserver in Android 4.4 and 5.1 before 5.1.1 LMY48X allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file.
Classification	Location : Remote Attack Type : Denial of Service, Arbitrary Code Execution, Buffer Overflow, Mem Impact : Loss of Confidentiality, Integrity, Availability Exploit Exploit :
Solution	Vendor updates are available. Please contact the vendor for more information.

Email: contact@varutra.com
Phone: +91 840 8891 911

Google Android up Mediaserver privilege escalation

General Details

Affected Version	5.1
Date of Publish	03-11-15
Varutra Vuln ID	KVA101
References	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8074
CVE ID	CVE-2015-8074
CVSSv2 Score	5

Vulnerability Summary

Vulnerability	Google Android up Mediaserver privilege escalation
Description	It was reported that the mediaserver in Android before 5.1.1 LMY48X allows remote attackers to obtain sensitive information, and consequently bypass an unspecified protection mechanism, via unknown vectors.
Classification	Location : Remote Attack Type : Bypass Security Restriction, Obtain Information, Privilege Escalati Impact : Loss of Confidentiality Exploit Exploit :
Solution	Vendor updates are available. Please contact the vendor for more information.

Google Android up Mediaserver buffer overflow

General Details

Affected Version	5.1.1
Date of Publish	03-11-15
Varutra Vuln ID	KVA102
References	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6608
CVE ID	CVE-2015-6608
CVSSv2 Score	10

Vulnerability Summary

Vulnerability	Google Android up Mediaserver buffer overflow
Description	It was reported that the mediaserver in Android 5.x before 5.1.1 LMY48X and 6.0 before 2015-11-01 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file.
Classification	Location : Remote Attack Type : Denial of Service, Arbitrary Code Execution, Buffer Overflow, Mem Impact : Loss of Confidentiality, Integrity, Availability Exploit Exploit :
Solution	Vendor updates are available. Please contact the vendor for more information.

Google Android up Mediaserver buffer overflow

General Details

Affected Version 5.1

Date of Publish	12/8/2015
Varutra Vuln ID	KVA103
References	http://source.android.com/security/bulletin/2015-12-01.html
CVE ID	CVE-2015-8505
CVSSv2 Score	9.3

Vulnerability Summary

Vulnerability	Google Android up Mediaserver buffer overflow
Description	It was reported that the mediaserver in Android before 5.1.1 LMY48Z allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file.
Classification	Location : Remote Attack Type : Denial of Service, Arbitrary Code Execution, Buffer Overflow, Mem Impact : Loss of Confidentiality, Integrity, Availability Exploit Exploit :
Solution	Vendor updates are available. Please contact the vendor for more information.

Google Android up Mediaserver buffer overflow

General Details

Affected Version	5.1, 6.0
Date of Publish	12/8/2015
Varutra Vuln ID	KVA104
References	http://source.android.com/security/bulletin/2015-12-01.html
CVE ID	CVE-2015-8506
CVSSv2 Score	9.3

Vulnerability Summary

Vulnerability	Google Android up Mediaserver buffer overflow
Description	It was reported that the mediaserver in Android before 5.1.1 LMY48Z and 6.0 before 2015-12-01 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file.
Classification	Location : Remote Attack Type : Denial of Service, Arbitrary Code Execution, Buffer Overflow, Mem Impact : Loss of Confidentiality, Integrity, Availability Exploit Exploit :
Solution	Vendor updates are available. Please contact the vendor for more information.

Google Android wpa_supplicant Denial of Service Vulnerability

General Details

Affected Version	4.4.4, 5.0, 5.1.1, 6.0, 6.0.1
Date of Publish	10-11-15
Varutra Vuln ID	KVA106
References	http://source.android.com/security/bulletin/2016-01-01.html
CVE ID	CVE-2015-5310
CVSSv2 Score	3.3

Vulnerability Summary

Vulnerability	Google Android wpa_supplicant Denial of Service Vulnerability
Description	It was reported that the Wi-Fi in Android before 5.1.1 LMY49F and 6.0 before 2016-01-01 allows remote attackers to obtain sensitive Wi-Fi information by leveraging access to the local physical environment.
Classification	Location : Remote Attack Type : Obtain Information Impact : Loss of Confidentiality Exploit Exploit :
Solution	Vendor updates are available. Please contact the vendor for more information.

Google Android Mediaserver Memory Corruption Vulnerability

General Details

Affected Version	5.0, 5.1.1, 6.0, 6.0.1
Date of Publish	04-01-16
Varutra Vuln ID	KVA107
References	http://source.android.com/security/bulletin/2016-01-01.html
CVE ID	CVE-2015-6636
CVSSv2 Score	10

Vulnerability Summary

Vulnerability	Google Android Mediaserver Memory Corruption Vulnerability
Description	It was reported that the mediaserver in Android 5.x before 5.1.1 LMY49F and 6.0 before 2016-01-01 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file.
Classification	Location : Remote Attack Type : Denial of Service, Arbitrary Code Execution, Buffer Overflow, Mem Impact : Loss of Confidentiality, Integrity, Availability Exploit Exploit :
Solution	Vendor updates are available. Please contact the vendor for more information.

Google Android 'misc-sd' driver Remote Privilege Escalation Vulnerability

General Details

Affected Version	4.4.4, 5.0, 5.1.1, 6.0, 6.0.1
Date of Publish	04-01-16
Varutra Vuln ID	KVA108
References	http://source.android.com/security/bulletin/2016-01-01.html
CVE ID	CVE-2015-6637
CVSSv2 Score	9.3

Vulnerability Summary

Vulnerability	Google Android 'misc-sd' driver Remote Privilege Escalation Vulnerability
Description	It was reported that the MediaTek misc-sd driver in Android before 5.1.1 LMY49F and 6.0 before 2016-01-01 allows attackers to gain privileges via a crafted application.
Classification	Location : Remote Attack Type : Gain Privileges Impact : Loss of Confidentiality, Integrity, Availability Exploit Exploit :
Solution	Vendor updates are available. Please contact the vendor for more information.

Email: contact@varutra.com
Phone: +91 840 8891 911

Google Android 'kernel' driver Remote Privilege Escalation Vulnerability

General Details

Affected Version	5.0, 5.1.1, 6.0, 6.0.1
Date of Publish	04-01-16
Varutra Vuln ID	KVA109
References	http://source.android.com/security/bulletin/2016-01-01.html
CVE ID	CVE-2015-6638
CVSSv2 Score	9.3

Vulnerability Summary

Vulnerability	Google Android 'kernel' driver Remote Privilege Escalation Vulnerability
Description	It was reported that the Imagination Technologies driver in Android 5.x before 5.1.1 LMY49F and 6.0 before 2016-01-01 allows attackers to gain privileges via a crafted application.
Classification	Location : Remote Attack Type : Gain Privileges Impact : Loss of Confidentiality, Integrity, Availability Exploit Exploit :
Solution	Vendor updates are available. Please contact the vendor for more information.

Google Android Widevine QSEE TrustZone Multiple Privilege Escalation Vulnerabilities

General Details

Affected Version	5.0, 5.1.1, 6.0, 6.0.1
Date of Publish	04-01-16
Varutra Vuln ID	KVA110
References	http://source.android.com/security/bulletin/2016-01-01.html
CVE ID	CVE-2015-6639
CVSSv2 Score	9.3

Vulnerability Summary

Vulnerability	Google Android Widevine QSEE TrustZone Multiple Privilege Escalation Vulnerabilities
Description	It was reported that the Widevine QSEE TrustZone application in Android 5.x before 5.1.1 LMY49F and 6.0 before 2016-01-01 allows attackers to gain privileges via a crafted application that leverages QSEECOM access.
Classification	Location : Remote Attack Type : Gain Privileges Impact : Loss of Confidentiality, Integrity, Availability Exploit Exploit :
Solution	Vendor updates are available. Please contact the vendor for more information.

Google Android Kernel Remote Privilege Escalation Vulnerability

General Details

Affected Version	4.4.4, 5.0, 5.1.1, 6.0
Date of Publish	04-01-16
Varutra Vuln ID	KVA111
References	http://source.android.com/security/bulletin/2016-01-01.html
CVE ID	CVE-2015-6640
CVSSv2 Score	9.3

Vulnerability Summary

Vulnerability	Google Android Kernel Remote Privilege Escalation Vulnerability
Description	It was reported that the prctl_set_vma_anon_name function in kernel/sys.c in Android before 5.1.1 LMY49F and 6.0 before 2016-01-01 does not ensure that only one vma is accessed in a certain update action, which allows attackers to gain privileges or cause a denial of service (vma list corruption) via a crafted application.
Classification	Location : Remote Attack Type : Denial of Service, Gain Privileges Impact : Loss of Confidentiality, Integrity, Availability Exploit Exploit :
Solution	Vendor updates are available. Please contact the vendor for more information.

Google Android Kernel Remote Privilege Escalation Vulnerability

General Details

Affected Version	5.1.0, 6.0, 6.0.1
Date of Publish	04-01-16
Varutra Vuln ID	KVA113
References	http://source.android.com/security/bulletin/2016-01-01.html
CVE ID	CVE-2015-6642
CVSSv2 Score	7.8

Vulnerability Summary

Vulnerability	Google Android Kernel Remote Privilege Escalation Vulnerability
Description	It was reported that the kernel in Android before 5.1.1 LMY49F and 6.0 before 2016-01-01 allows attackers to obtain sensitive information, and consequently bypass an unspecified protection mechanism, via unknown vectors, as demonstrated by obtaining Signature or SignatureOrSystem access.
Classification	Location : Remote Attack Type : Bypass Security Restriction, Obtain Information Impact : Loss of Confidentiality Exploit Exploit :
Solution	Vendor updates are available. Please contact the vendor for more information.

Google Android Local Privilege Escalation Vulnerability

General Details

Affected Version	5.1.1, 6.0, 6.0.1
Date of Publish	04-01-16
Varutra Vuln ID	KVA114
References	http://source.android.com/security/bulletin/2016-01-01.html
CVE ID	CVE-2015-6643
CVSSv2 Score	7.2

Vulnerability Summary

Vulnerability	Google Android Local Privilege Escalation Vulnerability
Description	It was observed that the Setup Wizard in Android 5.x before 5.1.1 LMY49F and 6.0 before 2016-01-01 allows physically proximate attackers to modify settings or bypass a reset protection mechanism via unspecified vectors.
Classification	Location : Local Attack Type : Bypass Security Restriction Impact : Loss of Confidentiality, Integrity, Availability Exploit Exploit :
Solution	Vendor updates are available. Please contact the vendor for more information.

Google Android Bouncy Castle Information Disclosure Vulnerability

General Details

Affected Version	4.4.4, 5.0, 5.0.1, 5.0.2, 5.1.0, 5.1.1, 6.0, 6.0.1
Date of Publish	04-01-16
Varutra Vuln ID	KVA115
References	http://source.android.com/security/bulletin/2016-01-01.html
CVE ID	CVE-2015-6644
CVSSv2 Score	4.3

Vulnerability Summary

Vulnerability	Google Android Bouncy Castle Information Disclosure Vulnerability
Description	It was observed that the Bouncy Castle in Android before 5.1.1 LMY49F and 6.0 before 2016-01-01 allows attackers to obtain sensitive information via a crafted application.
Classification	Location : Remote Attack Type : Obtain Information Impact : Loss of Confidentiality Exploit Exploit :
Solution	Vendor updates are available. Please contact the vendor for more information.

Email: contact@varutra.com
Phone: +91 840 8891 911

Google Android SyncManager Denial of Service Vulnerability

General Details

Affected Version	4.4.4, 5.0, 5.0.1, 5.0.2, 5.1.0, 5.1.1, 6.0
Date of Publish	04-01-16
Varutra Vuln ID	KVA116
References	http://source.android.com/security/bulletin/2016-01-01.html
CVE ID	CVE-2015-6645
CVSSv2 Score	7.1

Vulnerability Summary

Vulnerability	Google Android SyncManager Denial of Service Vulnerability
Description	It was observed that the SyncManager in Android before 5.1.1 LMY49F and 6.0 before 2016-01-01 allows attackers to cause a denial of service (continuous rebooting) via a crafted application.
Classification	Location : Remote Attack Type : Denial of Service Impact : Loss of Availability Exploit Exploit :
Solution	Vendor updates are available. Please contact the vendor for more information.

Email: contact@varutra.com
Phone: +91 840 8891 911

Google Android Widevine QSEE TrustZone Multiple Privilege Escalation Vulnerabilities

General Details

Affected Version	5.0, 5.0.1, 5.0.2, 5.1.0, 5.1.1, 6.0
Date of Publish	04-01-16
Varutra Vuln ID	KVA118
References	http://source.android.com/security/bulletin/2016-01-01.html
CVE ID	CVE-2015-6647
CVSSv2 Score	9.3

Vulnerability Summary

Vulnerability	Google Android Widevine QSEE TrustZone Multiple Privilege Escalation Vulnerabilities
Description	It was observed that the Widevine QSEE TrustZone application in Android 5.x before 5.1.1 LMY49F and 6.0 before 2016-01-01 allows attackers to gain privileges via a crafted application that leverages QSEECOM access.
Classification	Location : Remote Attack Type : Gain privileges Impact : Loss of Confidentiality, Integrity, Availability Exploit Exploit :
Solution	Vendor updates are available. Please contact the vendor for more information.

Google Android libcutils 'native_handle_ create()' Function Integer Overflow Vulnerability

General Details

Affected Version 5.1

Date of Publish	30-09-15
Varutra Vuln ID	KVA41
References	https://android.googlesource.com/platform/frameworks/native/+/7dcd0ec9c9168
CVE ID	CVE-2015-1528
CVSSv2 Score	9.3

Vulnerability Summary

Vulnerability

Google Android libcutils 'native_handle_ create()' Function Integer Overflow Vulnerability

Description

It was reported that an integer overflow in the native_handle_create function in libcutils/native_handle.c in Android before 5.1.1 LMY48M allows attackers to obtain a different application's privileges or cause a denial of service (Binder heap memory corruption) via a crafted application.

Classification

Location : Remote

Attack Type : Denial of Service, Buffer Overflow, Memory Corruption

Impact : Loss of Confidentiality, Integrity, Availability Exploit

Exploit :

Solution

Vendor updates are available. Please contact the vendor for more information.

Google Android Bitmap.cpp Bitmap_createFromParcel buffer overflow

General Details

Affected Version	5.1
Date of Publish	30-09-15
Varutra Vuln ID	KVA42
References	https://groups.google.com/forum/message/raw?msg=android-security-updates/U
CVE ID	CVE-2015-1536
CVSSv2 Score	8.5

Vulnerability Summary

Vulnerability	Google Android Bitmap.cpp Bitmap_createFromParcel buffer overflow
Description	It was reported that an integer overflow in the Bitmap_createFromParcel function in core/jni/android/graphics/Bitmap.cpp in Android before 5.1.1, LMY48I allows attackers to cause a denial of service (system_server crash) or obtain sensitive system_server memory-content information via a crafted application that leverages improper unmarshalling of bitmaps.
Classification	Location : Remote Attack Type : Denial of Service, Buffer Overflow, Obtain Information Impact : Loss of Confidentiality, Availability Exploit Exploit :
Solution	Vendor updates are available. Please contact the vendor for more information.

Email: contact@varutra.com
Phone: +91 840 8891 911

Google Stagefright Media Playback Engine Multiple Remote Code Execution Vulnerabilities

General Details

Affected Version	5.1
Date of Publish	30-09-15
Varutra Vuln ID	KVA43
References	https://android.googlesource.com/platform/frameworks/av/+/2434839bbd168469
CVE ID	CVE-2015-1538
CVSSv2 Score	10

Vulnerability Summary

Vulnerability	Google Stagefright Media Playback Engine Multiple Remote Code Execution Vulnerabilities
Description	It was reported that an integer overflow in the SampleTable::setSampleToChunkParams function in SampleTable.cpp in libstagefright in Android before 5.1.1 LMY48I allows remote attackers to execute arbitrary code via crafted atoms in MP4 data that trigger an unchecked multiplication.
Classification	Location : Remote Attack Type : Arbitrary Code Execution, Overflow Impact : Loss of Confidentiality, Integrity, Availability Exploit Exploit :
Solution	Vendor updates are available. Please contact the vendor for more information.

Google Stagefright Media Playback Engine Multiple Remote Code Execution Vulnerabilities

General Details

Affected Version 5.1

Date of Publish	30-09-15
Varutra Vuln ID	KVA44
References	https://android.googlesource.com/platform/frameworks/av/+/5e751957ba692658
CVE ID	CVE-2015-1539
CVSSv2 Score	10

Vulnerability Summary

Vulnerability

Google Stagefright Media Playback Engine Multiple Remote Code Execution Vulnerabilities

Description

It was reported that multiple integer underflows in the ESDS::parseESDescriptor function in ESDS.cpp in libstagefright in Android before 5.1.1 LMY48I allow remote attackers to execute arbitrary code.

Classification

Location : Remote

Attack Type : Arbitrary Code Execution

Impact : Loss of Confidentiality, Integrity, Availability Exploit

Exploit :

Solution

Vendor updates are available. Please contact the vendor for more information.

Email: contact@varutra.com
Phone: +91 840 8891 911

Google Android AppWidgetServiceImpl AppWidgetServiceImpl.java privilege escalation

General Details

Affected Version	5.1
Date of Publish	30-09-15
Varutra Vuln ID	KVA45
References	https://groups.google.com/forum/message/raw?msg=android-security-updates/U
CVE ID	CVE-2015-1541
CVSSv2 Score	4.3

Vulnerability Summary

Vulnerability	Google Android AppWidgetServiceImpl AppWidgetServiceImpl.java privilege escalation
Description	It was reported that the AppWidgetServiceImpl implementation in com/android/server/appwidget/AppWidgetServiceImpl.java in the Settings application in Android before 5.1.1 LMY48I allows attackers to obtain a URI permission via an application that sends an Intent with a (1) FLAG_GRANT_READ_URI_PERMISSION or (2) FLAG_GRANT_WRITE_URI_PERMISSION flag, as demonstrated by bypassing intended restrictions on reading contacts.
Classification	Location : Remote Attack Type : Bypass Security Restriction Impact : Loss of Confidentiality Exploit Exploit :
Solution	Vendor updates are available. Please contact the vendor for more information.

Email: contact@varutra.com
Phone: +91 840 8891 911

Google Android Integer Overflow Vulnerability

General Details

Affected Version 5.1

Date of Publish	07-10-15
Varutra Vuln ID	KVA46
References	http://www.securityfocus.com/bid/76165
CVE ID	CVE-2015-3823
CVSSv2 Score	10

Vulnerability Summary

Vulnerability	Google Android Integer Overflow Vulnerability
Description	It was reported that the libstagefright in Android before 5.1.1 LMY48T allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file.
Classification	Location : Remote Attack Type : Denial of Service, Arbitrary Code Execution, Buffer Overflow, Mem Impact : Loss of Confidentiality, Integrity, Availability Exploit Exploit :
Solution	Vendor updates are available. Please contact the vendor for more information.

Google Stagefright Media Playback Engine Multiple Remote Code Execution Vulnerabilities

General Details

Affected Version 5.1

Date of Publish	30-09-15
Varutra Vuln ID	KVA47
References	https://android.googlesource.com/platform/frameworks/av/+/463a6f807e187828
CVE ID	CVE-2015-3824
CVSSv2 Score	10

Vulnerability Summary

Vulnerability	Google Stagefright Media Playback Engine Multiple Remote Code Execution Vulnerabilities
Description	It was reported that the MPEG4Extractor::parseChunk function in MPEG4Extractor.cpp in libstagefright in Android before 5.1.1 LMY48I does not properly restrict size addition, which allows remote attackers to execute arbitrary code or cause a denial of service (integer overflow and memory corruption) via a crafted MPEG-4 tx3g atom.
Classification	Location : Remote Attack Type : Denial of Service, Arbitrary Code Execution, Buffer Overflow, Mem Impact : Loss of Confidentiality, Integrity, Availability Exploit Exploit :
Solution	Vendor updates are available. Please contact the vendor for more information.

Google Stagefright Media Playback Engine Multiple Remote Code Execution Vulnerabilities

General Details

Affected Version	5.1
Date of Publish	30-09-15
Varutra Vuln ID	KVA48
References	https://android.googlesource.com/platform/frameworks/av/+/f4f7e0c102819f039e
CVE ID	CVE-2015-3826
CVSSv2 Score	5

Vulnerability Summary

Vulnerability

Google Stagefright Media Playback Engine Multiple Remote Code Execution Vulnerabilities

Description

It was reported that the MPEG4Extractor::parse3GPPMetaData function in MPEG4Extractor.cpp in libstagefright in Android before 5.1.1 LMY48I does not enforce a minimum size for UTF-16 strings containing a Byte Order Mark (BOM), which allows remote attackers to cause a denial of service (integer underflow, buffer over-read, and mediaserver process crash) via crafted 3GPP metadata, aka internal bug 20923261.

Classification

Location : Remote

Attack Type : Denial of Service, Buffer Overflow

Impact : Loss of Availability Exploit

Exploit :

Solution

Vendor updates are available. Please contact the vendor for more information.

Google Stagefright Media Playback Engine Multiple Remote Code Execution Vulnerabilities

General Details

Affected Version	5.1
Date of Publish	30-09-15
Varutra Vuln ID	KVA49
References	https://android.googlesource.com/platform/frameworks/av/+/f4a88c8ed4f8186b3
CVE ID	CVE-2015-3827
CVSSv2 Score	9.3

Vulnerability Summary

Vulnerability

Google Stagefright Media Playback Engine Multiple Remote Code Execution Vulnerabilities

Description

It was reported that the MPEG4Extractor::parseChunk function in MPEG4Extractor.cpp in libstagefright in Android before 5.1.1 LMY48I does not validate the relationship between chunk sizes and skip sizes, which allows remote attackers to execute arbitrary code or cause a denial of service (integer underflow and memory corruption) via crafted MPEG-4 covr atoms, aka internal bug 20923261.

Classification

Location : Remote

Attack Type : Denial of Service, Arbitrary Code Execution, Buffer Overflow, Mem

Impact : Loss of Confidentiality, Integrity, Availability Exploit

Exploit :

Solution

Vendor updates are available. Please contact the vendor for more information.

Google Stagefright Media Playback Engine Multiple Remote Code Execution Vulnerabilities

General Details

Affected Version	5.1
Date of Publish	30-09-15
Varutra Vuln ID	KVA50
References	https://android.googlesource.com/platform/frameworks/av/+/f4f7e0c102819f039e
CVE ID	CVE-2015-3828
CVSSv2 Score	10

Vulnerability Summary

Vulnerability

Google Stagefright Media Playback Engine Multiple Remote Code Execution Vulnerabilities

Description

It was reported that the MPEG4Extractor::parse3GPPMetaData function in MPEG4Extractor.cpp in libstagefright in Android before 5.1.1 LMY48I does not enforce a minimum size for UTF-16 strings containing a Byte Order Mark (BOM), which allows remote attackers to execute arbitrary code or cause a denial of service (integer underflow and memory corruption) via crafted 3GPP metadata, aka internal bug 20923261.

Classification

Location : Remote

Attack Type : Denial of Service, Arbitrary Code Execution, Buffer Overflow, Mem

Impact : Loss of Confidentiality, Integrity, Availability Exploit

Exploit :

Solution

Vendor updates are available. Please contact the vendor for more information.

Google Stagefright Media Playback Engine Multiple Remote Code Execution Vulnerabilities

General Details

Affected Version	5.1
Date of Publish	30-09-15
Varutra Vuln ID	KVA51
References	https://android.googlesource.com/platform/frameworks/av/+/2674a7218eaa3c87
CVE ID	CVE-2015-3829
CVSSv2 Score	10

Vulnerability Summary

Vulnerability	Google Stagefright Media Playback Engine Multiple Remote Code Execution Vulnerabilities
Description	It was reported that Off-by-one error in the MPEG4Extractor::parseChunk function in MPEG4Extractor.cpp in libstagefright in Android before 5.1.1 LMY48I allows remote attackers to execute arbitrary code or cause a denial of service (integer overflow and memory corruption) via crafted MPEG-4 covr atoms with a size equal to SIZE_MAX.
Classification	Location : Remote Attack Type : Denial of Service, Arbitrary Code Execution, Buffer Overflow, Mem Impact : Loss of Confidentiality, Integrity, Availability Exploit Exploit :
Solution	Vendor updates are available. Please contact the vendor for more information.

Google Android BpMediaHTTPConnection IMediaHTTPConnection.cpp readAt buffer overflow

General Details

Affected Version	5.1
Date of Publish	30-09-15
Varutra Vuln ID	KVA52
References	https://groups.google.com/forum/message/raw?msg=android-security-updates/U
CVE ID	CVE-2015-3831
CVSSv2 Score	9.3

Vulnerability Summary

Vulnerability	Google Android BpMediaHTTPConnection IMediaHTTPConnection.cpp readAt buffer overflow
Description	It was reported that a Buffer overflow in the readAt function in BpMediaHTTPConnection in media/libmedia/IMediaHTTPConnection.cpp in the mediaserver service in Android before 5.1.1 LMY48I allows attackers to execute arbitrary code via a crafted application.
Classification	Location : Remote Attack Type : Arbitrary Code Execution, Buffer Overflow Impact : Loss of Confidentiality, Integrity, Availability Exploit Exploit :
Solution	Vendor updates are available. Please contact the vendor for more information.

Google Android libstagefright MPEG4Extractor.cpp MP4 File buffer overflow

General Details

Affected Version 5.1

Date of Publish	30-09-15
Varutra Vuln ID	KVA53
References	https://android.googlesource.com/platform/frameworks/av/+/d48f0f145f8f0f4472
CVE ID	CVE-2015-3832
CVSSv2 Score	10

Vulnerability Summary

Vulnerability

Google Android libstagefright MPEG4Extractor.cpp MP4 File buffer overflow

Description

It was reported that multiple buffer overflows in MPEG4Extractor.cpp in libstagefright in Android before 5.1.1 LMY48I allow remote attackers to execute arbitrary code via invalid size values of NAL units in MP4 data.

Classification

Location : Remote

Attack Type : Arbitrary Code Execution, Buffer Overflow

Impact : Loss of Confidentiality, Integrity, Availability Exploit

Exploit :

Solution

Vendor updates are available. Please contact the vendor for more information.

Google Android Java ActivityManagerService.java getRunningAppProcesses information disclosure

General Details

Affected Version	5.1
Date of Publish	30-09-15
Varutra Vuln ID	KVA54
References	https://groups.google.com/forum/message/raw?msg=android-security-updates/U
CVE ID	CVE-2015-3833
CVSSv2 Score	4.3

Vulnerability Summary

Vulnerability	Google Android Java ActivityManagerService.java getRunningAppProcesses information disclosure
Description	It was reported that the getRunningAppProcesses function in services/core/java/com/android/server/am/ActivityManagerService.java in Android before 5.1.1 LMY48I allows attackers to bypass intended getRecentTasks restrictions and discover the name of the foreground application via a crafted application.
Classification	Location : Remote Attack Type : Bypass Security Restriction, Information Disclosure Impact : Loss of Confidentiality Exploit Exploit :
Solution	Vendor updates are available. Please contact the vendor for more information.

Email: contact@varutra.com
Phone: +91 840 8891 911

Google Android media/libmedia/IHDCP.cpp BnHDCP::onTransact buffer overflow

General Details

Affected Version	5.1
Date of Publish	30-09-15
Varutra Vuln ID	KVA55
References	https://groups.google.com/forum/message/raw?msg=android-security-updates/U
CVE ID	CVE-2015-3834
CVSSv2 Score	10

Vulnerability Summary

Vulnerability

Google Android media/libmedia/IHDCP.cpp BnHDCP::onTransact buffer overflow

Description

It was reported that multiple integer overflows in the BnHDCP::onTransact function in media/libmedia/IHDCP.cpp in libstagefright in Android before 5.1.1 LMY48I allow attackers to execute arbitrary code via a crafted application that uses HDCP encryption, leading to a heap-based buffer overflow.

Classification

Location : Remote

Attack Type : Arbitrary Code Execution, Buffer Overflow

Impact : Loss of Confidentiality, Integrity, Availability Exploit

Exploit :

Solution

Vendor updates are available. Please contact the vendor for more information.

Google Android libstagefright omx/OMXNodeInstance.cpp emptyBuffer buffer overflow

General Details

Affected Version	5.1
Date of Publish	30-09-15
Varutra Vuln ID	KVA56
References	https://android.googlesource.com/platform/frameworks/av/+/086d84f45ab7b64d
CVE ID	CVE-2015-3835
CVSSv2 Score	9.3

Vulnerability Summary

Vulnerability

Google Android libstagefright omx/OMXNodeInstance.cpp emptyBuffer buffer overflow

Description

It was reported that a buffer overflow in the OMXNodeInstance::emptyBuffer function in omx/OMXNodeInstance.cpp in libstagefright in Android before 5.1.1 LMY48I allows attackers to execute arbitrary code via a crafted application.

Classification

Location : Remote

Attack Type : Arbitrary Code Execution, Buffer Overflow

Impact : Loss of Confidentiality, Integrity, Availability Exploit

Exploit :

Solution

Vendor updates are available. Please contact the vendor for more information.

Google Android Sonivox DLS-to-EAS Converter eas_mdls.c Parse_wave XMF Data buffer overflow

General Details

Affected Version	5.1
Date of Publish	30-09-15
Varutra Vuln ID	KVA57
References	https://android.googlesource.com/platform/external/sonivox/+/e999f077f6ef59d2
CVE ID	CVE-2015-3836
CVSSv2 Score	10

Vulnerability Summary

Vulnerability

Google Android Sonivox DLS-to-EAS Converter eas_mdls.c Parse_wave XMF Data buffer overflow

Description

It was reported that the Parse_wave function in arm-wt-22k/lib_src/eas_mdls.c in the Sonivox DLS-to-EAS converter in Android before 5.1.1 LMY48I does not reject a negative value for a certain size field, which allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow) via crafted XMF data.

Classification

Location : Remote

Attack Type : Denial of Service, Arbitrary Code Execution, Buffer Overflow

Impact : Loss of Confidentiality, Integrity, Availability Exploit

Exploit :

Solution

Vendor updates are available. Please contact the vendor for more information.

Google Android OpenSSLX509Certificate.java OpenSSLX509Certificate buffer overflow

General Details

Affected Version	5.1
Date of Publish	30-09-15
Varutra Vuln ID	KVA58
References	https://android.googlesource.com/platform/external/conscrypt/+/edf7055461e2d
CVE ID	CVE-2015-3837
CVSSv2 Score	9.3

Vulnerability Summary

Vulnerability	Google Android OpenSSLX509Certificate.java OpenSSLX509Certificate buffer overflow
Description	It was reported that the OpenSSLX509Certificate class in org/conscrypt/OpenSSLX509Certificate.java in Android before 5.1.1 LMY48I improperly includes certain context data during serialization and deserialization, which allows attackers to execute arbitrary code via an application that sends a crafted Intent.
Classification	Location : Remote Attack Type : Arbitrary Code Execution Impact : Loss of Confidentiality, Integrity, Availability Exploit Exploit :
Solution	Vendor updates are available. Please contact the vendor for more information.

Google Android Mediaserver buffer overflow

General Details

Affected Version	5.1
Date of Publish	30-09-15
Varutra Vuln ID	KVA59
References	https://android.googlesource.com/platform/frameworks/av/+/aeea52da00d21058
CVE ID	CVE-2015-3842
CVSSv2 Score	9.3

Vulnerability Summary

Vulnerability	Google Android Mediaserver buffer overflow
Description	It was reported that multiple heap-based buffer overflows in libeffects in the Audio Policy Service in mediaserver in Android before 5.1.1 LMY48I allow attackers to execute arbitrary code via a crafted application.
Classification	Location : Remote Attack Type : Arbitrary Code Execution, Buffer Overflow Impact : Loss of Confidentiality, Integrity, Availability Exploit Exploit :
Solution	Vendor updates are available. Please contact the vendor for more information.

Email: contact@varutra.com
Phone: +91 840 8891 911

Google Android SIM Toolkit Framework AppInterface.java privilege escalation

General Details

Affected Version 5.1

Date of Publish	30-09-15
Varutra Vuln ID	KVA60
References	https://android.googlesource.com/platform/packages/services/Telephony/+/fcb1
CVE ID	CVE-2015-3843
CVSSv2 Score	9.3

Vulnerability Summary

Vulnerability

Google Android SIM Toolkit Framework AppInterface.java privilege escalation

Description

It was reported that the SIM Toolkit (STK) framework in Android before 5.1.1 LMY48I allows attackers to (1) intercept or (2) emulate unspecified Telephony STK SIM commands via an application that sends a crafted Intent, related to com/android/internal/telephony/cat/AppInterface.java.

Classification

Location : Remote

Attack Type : Privilege Escalation

Impact : Loss of Confidentiality, Integrity, Availability Exploit

Exploit :

Solution

Vendor updates are available. Please contact the vendor for more information.

Google Android ActivityManagerService.java getProcessRecordLocked privilege escalation

General Details

Affected Version	5.1
Date of Publish	30-09-15
Varutra Vuln ID	KVA61
References	https://android.googlesource.com/platform/frameworks/base/+/e3cde784e3d999
CVE ID	CVE-2015-3844
CVSSv2 Score	6.8

Vulnerability Summary

Vulnerability

Google Android ActivityManagerService.java getProcessRecordLocked privilege escalation

Description

It was reported that the getProcessRecordLocked method in services/core/java/com/android/server/am/ActivityManagerService.java in ActivityManager in Android before 5.1.1 LMY48I allows attackers to trigger incorrect process loading via a crafted application, as demonstrated by interfering with use of the Settings application.

Classification

Location : Remote

Attack Type : Privilege Escalation

Impact : Loss of Confidentiality, Integrity, Availability Exploit

Exploit :

Solution

Vendor updates are available. Please contact the vendor for more information.

Google Android Binder libs/binder/Parcel.cpp Parcel::appendFrom privilege escalation

General Details

Affected Version	5.1
Date of Publish	30-09-15
Varutra Vuln ID	KVA62
References	https://android.googlesource.com/platform/frameworks/native/+/e68cbc3e9e66d
CVE ID	CVE-2015-3845
CVSSv2 Score	6.8

Vulnerability Summary

Vulnerability	Google Android Binder libs/binder/Parcel.cpp Parcel::appendFrom privilege escalation
Description	It was reported that the Parcel::appendFrom function in libs/binder/Parcel.cpp in Binder in Android before 5.1.1 LMY48M does not consider parcel boundaries during identification of binder objects in an append operation, which allows attackers to obtain a different application's privileges via a crafted application.
Classification	Location : Remote Attack Type : Privilege Escalation Impact : Loss of Confidentiality, Integrity, Availability Exploit Exploit :
Solution	Vendor updates are available. Please contact the vendor for more information.

Email: contact@varutra.com
Phone: +91 840 8891 911

Google Android Bluetooth denial of service

General Details

Affected Version 5.1

Date of Publish	06-10-15
Varutra Vuln ID	KVA63
References	https://groups.google.com/forum/#!msg/android-security-updates/iv1BF0f0XY4/3
CVE ID	CVE-2015-3847
CVSSv2 Score	6.4

Vulnerability Summary

Vulnerability: Google Android Bluetooth denial of service

Description: It was reported that Bluetooth in Android before 5.1.1 LMY48T allows attackers to remove stored SMS messages via a crafted application.

Classification:
Location : Remote
Attack Type : Denial of Service
Impact : Loss of Integrity, Availability Exploit
Exploit :

Solution: Vendor updates are available. Please contact the vendor for more information.

Google Android Arbitrary remote code execution Vulnerability

General Details

Affected Version	5.1
Date of Publish	30-09-15
Varutra Vuln ID	KVA64
References	https://groups.google.com/forum/message/raw?msg=android-security-updates/1
CVE ID	CVE-2015-3849
CVSSv2 Score	9.3

Vulnerability Summary

Vulnerability	Google Android Arbitrary remote code execution Vulnerability
Description	It was reported that the Region_createFromParcel function in core/jni/android/graphics/Region.cpp in Region in Android before 5.1.1 LMY48M does not check the return values of certain read operations, which allows attackers to execute arbitrary code via an application that sends a crafted message to a service.
Classification	Location : Remote Attack Type : Arbitrary Code Execution Impact : Loss of Confidentiality, Integrity, Availability Exploit Exploit :
Solution	Vendor updates are available. Please contact the vendor for more information.

Google Android SMSDispatcher.java checkDestination privilege escalation

General Details

Affected Version	5.1
Date of Publish	30-09-15
Varutra Vuln ID	KVA65
References	https://groups.google.com/forum/message/raw?msg=android-security-updates/1
CVE ID	CVE-2015-3858
CVSSv2 Score	9.3

Vulnerability Summary

Vulnerability	Google Android SMSDispatcher.java checkDestination privilege escalation
Description	It was reported that the checkDestination function in internal/telephony/SMSDispatcher.java in Android before 5.1.1 LMY48M relies on an obsolete permission name for an authorization check, which allows attackers to bypass an intended user-confirmation requirement for SMS short-code messaging via a crafted application.
Classification	Location : Remote Attack Type : Bypass Security Restriction Impact : Loss of Confidentiality, Integrity, Availability Exploit Exploit :
Solution	Vendor updates are available. Please contact the vendor for more information.

Google Android Lock Screen Security Bypass Vulnerability

General Details

Affected Version	5.1
Date of Publish	30-09-15
Varutra Vuln ID	KVA66
References	https://code.google.com/p/android/issues/detail?id=178139
CVE ID	CVE-2015-3860
CVSSv2 Score	7.2

Vulnerability Summary

Vulnerability	Google Android Lock Screen Security Bypass Vulnerability
Description	It was reported that packages/Keyguard/res/layout/keyguard_password_view.xml in Lockscreen in Android 5.x before 5.1.1 LMY48M does not restrict the number of characters in the passwordEntry input field, which allows physically proximate attackers to bypass intended access restrictions via a long password that triggers a SystemUI crash.
Classification	Location : Local Attack Type : Bypass Security Restriction Impact : Loss of Confidentiality, Integrity, Availability Exploit Exploit :
Solution	Vendor updates are available. Please contact the vendor for more information.

Google Android Mediaserver MatroskaExtractor.cpp addVorbisCodecInfo buffer overflow

General Details

Affected Version	5.1
Date of Publish	30-09-15
Varutra Vuln ID	KVA67
References	https://groups.google.com/forum/message/raw?msg=android-security-updates/1
CVE ID	CVE-2015-3861
CVSSv2 Score	5

Vulnerability Summary

Vulnerability	Google Android Mediaserver MatroskaExtractor.cpp addVorbisCodecInfo buffer overflow
Description	It was reported that multiple integer overflows in the addVorbisCodecInfo function in matroska/MatroskaExtractor.cpp in libstagefright in mediaserver in Android before 5.1.1 LMY48M allow remote attackers to cause a denial of service (device inoperability) via crafted Matroska data.
Classification	Location : Remote Attack Type : Denial of Service, Buffer Overflow Impact : Loss of Availability Exploit Exploit :
Solution	Vendor updates are available. Please contact the vendor for more information.

Email: contact@varutra.com
Phone: +91 840 8891 911

Google Android Mediaserver Crash denial of service

General Details

Affected Version	5.1
Date of Publish	06-10-15
Varutra Vuln ID	KVA68
References	https://groups.google.com/forum/#!topic/android-security-updates/iv1BF0f0XY4
CVE ID	CVE-2015-3862
CVSSv2 Score	5

Vulnerability Summary

Vulnerability	Google Android Mediaserver Crash denial of service
Description	It was observed that the mediaserver in Android before 5.1.1 LMY48T allows attackers to cause a denial of service (process crash) via unspecified vectors.
Classification	Location : Remote Attack Type : Denial of Service Impact : Loss of Availability Exploit Exploit :
Solution	Vendor updates are available. Please contact the vendor for more information.

Email: contact@varutra.com
Phone: +91 840 8891 911

Google Android Blob Class keystore/keystore.cpp buffer overflow

General Details

Affected Version 5.1

Date of Publish	30-09-15
Varutra Vuln ID	KVA69
References	https://groups.google.com/forum/message/raw?msg=android-security-updates/1
CVE ID	CVE-2015-3863
CVSSv2 Score	9.3

Vulnerability Summary

Vulnerability: Google Android Blob Class keystore/keystore.cpp buffer overflow

Description: It was reported that multiple integer overflows in the Blob class in keystore/keystore.cpp in Keystore in Android before 5.1.1 LMY48M allow attackers to execute arbitrary code and read arbitrary Keystore keys via an application that uses a crafted blob in an insert operation.

Classification:
Location : Remote
Attack Type : Arbitrary Code Execution, Buffer Overflow
Impact : Loss of Confidentiality, Integrity, Availability Exploit
Exploit :

Solution: Vendor updates are available. Please contact the vendor for more information.

Google Android Stagefright Incomplete Fix Integer Overflow Vulnerability

General Details

Affected Version 5.1

Date of Publish	30-09-15
Varutra Vuln ID	KVA70
References	https://groups.google.com/forum/message/raw?msg=android-security-updates/1
CVE ID	CVE-2015-3864
CVSSv2 Score	10

Vulnerability Summary

Vulnerability

Google Android Stagefright Incomplete Fix Integer Overflow Vulnerability

Description

It was reported that the integer underflow in the MPEG4Extractor::parseChunk function in MPEG4Extractor.cpp in libstagefright in mediaserver in Android before 5.1.1 LMY48M allows remote attackers to execute arbitrary code via crafted MPEG-4 data.

Classification

Location : Remote

Attack Type : Arbitrary Code Execution, Buffer Overflow

Impact : Loss of Confidentiality, Integrity, Availability Exploit

Exploit :

Solution

Vendor updates are available. Please contact the vendor for more information.

Email: contact@varutra.com
Phone: +91 840 8891 911

Google Android Runtime Subsystem privilege escalation

General Details

Affected Version	5.1
Date of Publish	06-10-15
Varutra Vuln ID	KVA71
References	https://groups.google.com/forum/#!msg/android-security-updates/iv1BF0f0XY4/3
CVE ID	CVE-2015-3865
CVSSv2 Score	9.3

Vulnerability Summary

Vulnerability	Google Android Runtime Subsystem privilege escalation
Description	It was reported that therRuntime subsystem in Android before 5.1.1 LMY48T allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access.
Classification	Location : Remote Attack Type : Gain Privileges Impact : Loss of Confidentiality, Integrity, Availability Exploit Exploit :
Solution	Vendor updates are available. Please contact the vendor for more information.

Google Android libstagefright buffer overflow Vulnerability

General Details

Affected Version 5.1

Date of Publish	06-10-15
Varutra Vuln ID	KVA72
References	https://groups.google.com/forum/#!msg/android-security-updates/iv1BF0f0XY4/3
CVE ID	CVE-2015-3867
CVSSv2 Score	10

Vulnerability Summary

Vulnerability: Google Android libstagefright buffer overflow Vulnerability

Description: It was reported that the libstagefright in Android before 5.1.1 LMY48T allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file.

Classification:
Location : Remote
Attack Type : Denial of Service, Arbitrary Code Execution, Buffer Overflow, Mem
Impact : Loss of Confidentiality, Integrity, Availability Exploit
Exploit :

Solution: Vendor updates are available. Please contact the vendor for more information.

Google Android libstagefright buffer overflow

General Details

Affected Version 5.1

Date of Publish	06-10-15
Varutra Vuln ID	KVA73
References	https://groups.google.com/forum/#!msg/android-security-updates/iv1BF0f0XY4/3
CVE ID	CVE-2015-3868
CVSSv2 Score	10

Vulnerability Summary

Vulnerability Google Android libstagefright buffer overflow

Description It was reported that the libstagefright in Android before 5.1.1 LMY48T allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file.

Classification
Location : Remote
Attack Type : Denial of Service, Arbitrary Code Execution, Buffer Overflow, Mem
Impact : Loss of Confidentiality, Integrity, Availability Exploit
Exploit :

Solution Vendor updates are available. Please contact the vendor for more information.

Email: contact@varutra.com
Phone: +91 840 8891 911

Google Android libstagefright buffer overflow

General Details

Affected Version 5.1

Date of Publish	06-10-15
Varutra Vuln ID	KVA74
References	https://groups.google.com/forum/#!msg/android-security-updates/iv1BF0f0XY4/3
CVE ID	CVE-2015-3869
CVSSv2 Score	10

Vulnerability Summary

Vulnerability Google Android libstagefright buffer overflow

Description It was reported that the libstagefright in Android before 5.1.1 LMY48T allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file.

Classification
Location : Remote
Attack Type : Denial of Service, Arbitrary Code Execution, Buffer Overflow, Mem
Impact : Loss of Confidentiality, Integrity, Availability Exploit
Exploit :

Solution Vendor updates are available. Please contact the vendor for more information.

Google Android libstagefright buffer overflow

General Details

Affected Version 5.1

Date of Publish	06-10-15
Varutra Vuln ID	KVA75
References	https://groups.google.com/forum/#!msg/android-security-updates/iv1BF0f0XY4/3
CVE ID	CVE-2015-3870
CVSSv2 Score	10

Vulnerability Summary

Vulnerability Google Android libstagefright buffer overflow

Description It was reported that the libstagefright in Android before 5.1.1 LMY48T allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file.

Classification
Location : Remote
Attack Type : Denial of Service, Arbitrary Code Execution, Buffer Overflow, Mem
Impact : Loss of Confidentiality, Integrity, Availability Exploit
Exploit :

Solution Vendor updates are available. Please contact the vendor for more information.

Google Android libstagefright buffer overflow

General Details

Affected Version 5.1

Date of Publish	06-10-15
Varutra Vuln ID	KVA76
References	https://groups.google.com/forum/#!msg/android-security-updates/iv1BF0f0XY4/3
CVE ID	CVE-2015-3871
CVSSv2 Score	10

Vulnerability Summary

Vulnerability Google Android libstagefright buffer overflow

Description It was reported that the libstagefright in Android before 5.1.1 LMY48T allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file.

Classification
Location : Remote
Attack Type : Denial of Service, Arbitrary Code Execution, Buffer Overflow, Mem
Impact : Loss of Confidentiality, Integrity, Availability Exploit
Exploit :

Solution Vendor updates are available. Please contact the vendor for more information.

Google Android libstagefright buffer overflow

General Details

Affected Version 5.1

Date of Publish	06-10-15
Varutra Vuln ID	KVA77
References	https://groups.google.com/forum/#!msg/android-security-updates/iv1BF0f0XY4/3
CVE ID	CVE-2015-3872
CVSSv2 Score	10

Vulnerability Summary

Vulnerability Google Android libstagefright buffer overflow

Description It was reported that the libstagefright in Android before 5.1.1 LMY48T allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file.

Classification
Location : Remote
Attack Type : Denial of Service, Arbitrary Code Execution, Buffer Overflow, Mem
Impact : Loss of Confidentiality, Integrity, Availability Exploit
Exploit :

Solution Vendor updates are available. Please contact the vendor for more information.

Google Android libstagefright buffer overflow

General Details

Affected Version 5.1

Date of Publish	06-10-15
Varutra Vuln ID	KVA78
References	https://groups.google.com/forum/#!msg/android-security-updates/iv1BF0f0XY4/3
CVE ID	CVE-2015-3873
CVSSv2 Score	10

Vulnerability Summary

Vulnerability Google Android libstagefright buffer overflow

Description It was reported that the libstagefright in Android before 5.1.1 LMY48T allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file.

Classification
Location : Remote
Attack Type : Denial of Service, Arbitrary Code Execution, Buffer Overflow, Mem
Impact : Loss of Confidentiality, Integrity, Availability Exploit
Exploit :

Solution Vendor updates are available. Please contact the vendor for more information.

Google Android Sonivox buffer overflow

General Details

Affected Version 5.1

Date of Publish	06-10-15
Varutra Vuln ID	KVA79
References	https://groups.google.com/forum/#!msg/android-security-updates/iv1BF0f0XY4/3
CVE ID	CVE-2015-3874
CVSSv2 Score	10

Vulnerability Summary

Vulnerability Google Android Sonivox buffer overflow

Description It was reported that the Sonivox components in Android before 5.1.1 LMY48T allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file.

Classification
Location : Remote
Attack Type : Denial of Service, Arbitrary Code Execution, Buffer Overflow, Mem
Impact : Loss of Confidentiality, Integrity, Availability Exploit
Exploit :

Solution Vendor updates are available. Please contact the vendor for more information.

Email: contact@varutra.com
Phone: +91 840 8891 911

Google Android libutils buffer overflow

General Details

Affected Version 5.1

Date of Publish	06-10-15
Varutra Vuln ID	KVA80
References	https://groups.google.com/forum/#!msg/android-security-updates/iv1BF0f0XY4/3
CVE ID	CVE-2015-3875
CVSSv2 Score	10

Vulnerability Summary

Vulnerability Google Android libutils buffer overflow

Description It was reported that the libutils in Android before 5.1.1 LMY48T allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted audio file.

Classification
Location : Remote
Attack Type : Denial of Service, Arbitrary Code Execution, Buffer Overflow, Mem
Impact : Loss of Confidentiality, Integrity, Availability Exploit
Exploit :

Solution Vendor updates are available. Please contact the vendor for more information.

Google Android libstagefright MP3/MP4 File buffer overflow

General Details

Affected Version 5.1.1

Date of Publish	01-10-15
Varutra Vuln ID	KVA81
References	https://groups.google.com/forum/#!msg/android-security-updates/iv1BF0f0XY4/3
CVE ID	CVE-2015-3876
CVSSv2 Score	9.3

Vulnerability Summary

Vulnerability: Google Android libstagefright MP3/MP4 File buffer overflow

Description: It was reported that the libstagefright in Android through 5.1.1 LMY48M allows remote attackers to execute arbitrary code via crafted metadata in a (1) MP3 or (2) MP4 file.

Classification:
Location : Remote
Attack Type : Arbitrary Code Execution, Buffer Overflow
Impact : Loss of Confidentiality, Integrity, Availability Exploit
Exploit :

Solution: Vendor updates are available. Please contact the vendor for more information.

Google Android Skia 20723696 buffer overflow

General Details

Affected Version 5.1

Date of Publish	06-10-15
Varutra Vuln ID	KVA82
References	https://groups.google.com/forum/#!msg/android-security-updates/iv1BF0f0XY4/3
CVE ID	CVE-2015-3877
CVSSv2 Score	10

Vulnerability Summary

Vulnerability Google Android Skia 20723696 buffer overflow

Description It was reported that the Skia, as used in Android before 5.1.1 LMY48T, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file.

Classification
Location : Remote
Attack Type : Denial of Service, Arbitrary Code Execution, Overflow, Memory Co
Impact : Loss of Confidentiality, Integrity, Availability Exploit
Exploit :

Solution Vendor updates are available. Please contact the vendor for more information.

Google Android Media Projection information disclosure

General Details

Affected Version	5.0, 5.1
Date of Publish	06-10-15
Varutra Vuln ID	KVA83
References	https://groups.google.com/forum/#!msg/android-security-updates/iv1BF0f0XY4/3
CVE ID	CVE-2015-3878
CVSSv2 Score	4.3

Vulnerability Summary

Vulnerability	Google Android Media Projection information disclosure
Description	It was reported that the media Projection in Android 5.x before 5.1.1 LMY48T and 6.0 before 2015-10-01 allows attackers to bypass an intended screen-recording warning feature and obtain sensitive screen-snapshot information via a crafted application that references a long application name.
Classification	Location : Remote Attack Type : Bypass Security Restriction, Obtain Information Impact : Loss of Confidentiality Exploit Exploit :
Solution	Vendor updates are available. Please contact the vendor for more information.

Email: contact@varutra.com
Phone: +91 840 8891 911

Google Android Media Player Framework privilege escalation

General Details

Affected Version	5.1
Date of Publish	06-10-15
Varutra Vuln ID	KVA84
References	https://groups.google.com/forum/#!msg/android-security-updates/iv1BF0f0XY4/3
CVE ID	CVE-2015-3879
CVSSv2 Score	9.3

Vulnerability Summary

Vulnerability	Google Android Media Player Framework privilege escalation
Description	It was reported that the Media Player Framework in Android before 5.1.1 LMY48T allows attackers to gain privileges via a crafted application.
Classification	Location : Remote Attack Type : Gain Privileges Impact : Loss of Confidentiality, Integrity, Availability Exploit Exploit :
Solution	Vendor updates are available. Please contact the vendor for more information.

Google Android libstagefright SampleTable.cpp MP4 File buffer overflow

General Details

Affected Version	5.1
Date of Publish	30-09-15
Varutra Vuln ID	KVA85
References	https://android.googlesource.com/platform/frameworks/av/+/cf1581c66c2ad8c5b
CVE ID	CVE-2015-6575
CVSSv2 Score	10

Vulnerability Summary

Vulnerability	Google Android libstagefright SampleTable.cpp MP4 File buffer overflow
Description	It was reported that the SampleTable.cpp in libstagefright in Android before 5.1.1 LMY48I does not properly consider integer promotion, which allows remote attackers to execute arbitrary code or cause a denial of service (integer overflow and memory corruption) via crafted atoms in MP4 data.
Classification	Location : Remote Attack Type : Denial of Service, Arbitrary Code Execution, Buffer Overflow, Mem Impact : Loss of Confidentiality, Integrity, Availability Exploit Exploit :
Solution	Vendor updates are available. Please contact the vendor for more information.

Google Android mediaserver privilege escalation

General Details

Affected Version	5.1
Date of Publish	06-10-15
Varutra Vuln ID	KVA86
References	https://groups.google.com/forum/#!msg/android-security-updates/iv1BF0f0XY4/3
CVE ID	CVE-2015-6596
CVSSv2 Score	9.3

Vulnerability Summary

Vulnerability	Google Android mediaserver privilege escalation
Description	It was reported that the mediaserver in Android before 5.1.1 LMY48T allows attackers to gain privileges via a crafted application.
Classification	Location : Remote Attack Type : Gain Privileges Impact : Loss of Confidentiality, Integrity, Availability Exploit Exploit :
Solution	Vendor updates are available. Please contact the vendor for more information.

Email: contact@varutra.com
Phone: +91 840 8891 911

Google Android libstagefright buffer overflow

General Details

Affected Version 5.1

Date of Publish	06-10-15
Varutra Vuln ID	KVA87
References	https://groups.google.com/forum/#!msg/android-security-updates/iv1BF0f0XY4/3
CVE ID	CVE-2015-6598
CVSSv2 Score	10

Vulnerability Summary

Vulnerability Google Android libstagefright buffer overflow

Description It was reported that the libstagefright in Android before 5.1.1 LMY48T allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file.

Classification
Location : Remote
Attack Type : Denial of Service, Arbitrary Code Execution, Memory Corruption
Impact : Loss of Confidentiality, Integrity, Availability Exploit
Exploit :

Solution Vendor updates are available. Please contact the vendor for more information.

Google Android libstagefright buffer overflow

General Details

Affected Version 5.1

Date of Publish	06-10-15
Varutra Vuln ID	KVA88
References	https://groups.google.com/forum/#!msg/android-security-updates/iv1BF0f0XY4/3
CVE ID	CVE-2015-6599
CVSSv2 Score	10

Vulnerability Summary

Vulnerability Google Android libstagefright buffer overflow

Description It was reported that the libstagefright in Android before 5.1.1 LMY48T allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file.

Classification
Location : Remote
Attack Type : Denial of Service, Arbitrary Code Execution, Buffer Overflow, Mem
Impact : Loss of Confidentiality, Integrity, Availability Exploit
Exploit :

Solution Vendor updates are available. Please contact the vendor for more information.

Google Android libstagefright buffer overflow

General Details

Affected Version 5.1

Date of Publish	06-10-15
Varutra Vuln ID	KVA89
References	https://groups.google.com/forum/#!msg/android-security-updates/iv1BF0f0XY4/3
CVE ID	CVE-2015-6600
CVSSv2 Score	10

Vulnerability Summary

Vulnerability Google Android libstagefright buffer overflow

Description It was reported that the libstagefright in Android before 5.1.1 LMY48T allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file.

Classification
Location : Remote
Attack Type : Denial of Service, Arbitrary Code Execution, Buffer Overflow, Mem
Impact : Loss of Confidentiality, Integrity, Availability Exploit
Exploit :

Solution Vendor updates are available. Please contact the vendor for more information.

Google Android libstagefright buffer overflow

General Details

Affected Version 5.1

Date of Publish	06-10-15
Varutra Vuln ID	KVA90
References	https://groups.google.com/forum/#!msg/android-security-updates/iv1BF0f0XY4/3
CVE ID	CVE-2015-6601
CVSSv2 Score	10

Vulnerability Summary

Vulnerability: Google Android libstagefright buffer overflow

Description: It was reported that the libstagefright in Android before 5.1.1 LMY48T allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file.

Classification:
Location : Remote
Attack Type : Denial of Service, Arbitrary Code Execution, Buffer Overflow, Mem
Impact : Loss of Confidentiality, Integrity, Availability Exploit
Exploit :

Solution: Vendor updates are available. Please contact the vendor for more information.

Google Android libutils MP3/MP4 File buffer overflow

General Details

Affected Version	5.1.1
Date of Publish	01-10-15
Varutra Vuln ID	KVA91
References	https://support.silentcircle.com/customer/en/portal/articles/2145864-privatos-1-1-
CVE ID	CVE-2015-6602
CVSSv2 Score	9.3

Vulnerability Summary

Vulnerability	Google Android libutils MP3/MP4 File buffer overflow
Description	It was reported that the libutils in Android through 5.1.1 LMY48M allows remote attackers to execute arbitrary code via crafted metadata in a (1) MP3 or (2) MP4 file, as demonstrated by an attack against use of libutils by libstagefright in Android 5.x.
Classification	Location : Remote Attack Type : Arbitrary Code Execution Impact : Loss of Confidentiality, Integrity, Availability Exploit Exploit :
Solution	Vendor updates are available. Please contact the vendor for more information.

Google Android libstagefright buffer overflow

General Details

Affected Version 5.1

Date of Publish	06-10-15
Varutra Vuln ID	KVA92
References	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6603
CVE ID	CVE-2015-6603
CVSSv2 Score	10

Vulnerability Summary

Vulnerability: Google Android libstagefright buffer overflow

Description: It was reported that the libstagefright in Android before 5.1.1 LMY48T allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file.

Classification:
Location : Remote
Attack Type : Denial of Service, Arbitrary Code Execution, Buffer Overflow, Mem
Impact : Loss of Confidentiality, Integrity, Availability Exploit
Exploit :

Solution: Vendor updates are available. Please contact the vendor for more information.

Google Android libstagefright buffer overflow

General Details

Affected Version	5.1
Date of Publish	06-10-15
Varutra Vuln ID	KVA93
References	https://groups.google.com/forum/#!msg/android-security-updates/iv1BF0f0XY4/3
CVE ID	CVE-2015-6604
CVSSv2 Score	10

Vulnerability Summary

Vulnerability	Google Android libstagefright buffer overflow
Description	It was reported that the libstagefright in Android before 5.1.1 LMY48T allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file.
Classification	Location : Remote Attack Type : Denial of Service, Arbitrary Code Execution, Buffer Overflow, Mem Impact : Loss of Confidentiality, Integrity, Availability Exploit Exploit :
Solution	Vendor updates are available. Please contact the vendor for more information.

Google Android Mediaserver Crash denial of service

General Details

Affected Version	5.1
Date of Publish	06-10-15
Varutra Vuln ID	KVA94
References	https://groups.google.com/forum/#!msg/android-security-updates/iv1BF0f0XY4/3
CVE ID	CVE-2015-6605
CVSSv2 Score	5

Vulnerability Summary

Vulnerability	Google Android Mediaserver Crash denial of service
Description	It was reported that the mediaserver in Android before 5.1.1 LMY48T allows attackers to cause a denial of service (process crash) via unspecified vectors.
Classification	Location : Remote Attack Type : Denial of Service Impact : Loss of Confidentiality Exploit Exploit :
Solution	Vendor updates are available. Please contact the vendor for more information.

Email: contact@varutra.com
Phone: +91 840 8891 911

Google Android Secure Element Evaluation Kit privilege escalation

General Details

Affected Version 5.1

Date of Publish	06-10-15
Varutra Vuln ID	KVA95
References	https://groups.google.com/forum/#!msg/android-security-updates/iv1BF0f0XY4/3
CVE ID	CVE-2015-6606
CVSSv2 Score	9.3

Vulnerability Summary

Vulnerability: Google Android Secure Element Evaluation Kit privilege escalation

Description: It was reported that the Secure Element Evaluation Kit (aka SEEK or SmartCard API) plugin in Android before 5.1.1 LMY48T allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access.

Classification:
Location : Remote
Attack Type : Gain Privileges
Impact : Loss of Confidentiality, Integrity, Availability Exploit
Exploit :

Solution: Vendor updates are available. Please contact the vendor for more information.

Google Android libstagefright buffer overflow

General Details

Affected Version 5.1

Date of Publish	06-10-15
Varutra Vuln ID	KVA96
References	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7716
CVE ID	CVE-2015-7716
CVSSv2 Score	10

Vulnerability Summary

Vulnerability: Google Android libstagefright buffer overflow

Description: It was reported that the libstagefright in Android 5.x before 5.1.1 LMY48T allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file.

Classification:
Location : Remote
Attack Type : Denial of Service, Arbitrary Code Execution, Buffer Overflow, Mem
Impact : Loss of Confidentiality, Integrity, Availability Exploit
Exploit :

Solution: Vendor updates are available. Please contact the vendor for more information.

Google Android Mediaserver privilege escalation

General Details

Affected Version	5.1
Date of Publish	06-10-15
Varutra Vuln ID	KVA97
References	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7717
CVE ID	CVE-2015-7717
CVSSv2 Score	9.3

Vulnerability Summary

Vulnerability	Google Android Mediaserver privilege escalation
Description	It was reported that the mediaserver in Android 5.x before 5.1.1 LMY48T and 6.0 before 2015-10-01 allows attackers to gain privileges via a crafted application.
Classification	Location : Remote Attack Type : Gain Privileges Impact : Loss of Confidentiality, Integrity, Availability Exploit Exploit :
Solution	Vendor updates are available. Please contact the vendor for more information.

Google Android Mediaserver Crash denial of service

General Details

Affected Version	5.1
Date of Publish	06-10-15
Varutra Vuln ID	KVA98
References	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7718
CVE ID	CVE-2015-7718
CVSSv2 Score	5

Vulnerability Summary

Vulnerability	Google Android Mediaserver Crash denial of service
Description	It was reported that the mediaserver in Android 5.x before 5.1.1 LMY48T and 6.0 before 2015-10-01 allows attackers to cause a denial of service (process crash) via unspecified vectors.
Classification	Location : Remote Attack Type : Denial of Service Impact : Loss of Availability Exploit Exploit :
Solution	Vendor updates are available. Please contact the vendor for more information.

Email: contact@varutra.com
Phone: +91 840 8891 911

Google Android up Mediaserver buffer overflow

General Details

Affected Version	4.4, 5.1
Date of Publish	03-11-15
Varutra Vuln ID	KVA99
References	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8072
CVE ID	CVE-2015-8072
CVSSv2 Score	10

Vulnerability Summary

Vulnerability	Google Android up Mediaserver buffer overflow
Description	It was reported that the mediaserver in Android 4.4 through 5.x before 5.1.1 LMY48X and 6.0 before 2015-11-01 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file.
Classification	Location : Remote Attack Type : Denial of Service, Arbitrary Code Execution, Buffer Overflow, Mem Impact : Loss of Confidentiality, Integrity, Availability Exploit Exploit :
Solution	Vendor updates are available. Please contact the vendor for more information.