CVE-2011-1823

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2011-1823
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-06-09 10:36:27 UTC
Updated	2026-04-21 20:29:52 UTC
Description	The vold volume manager daemon on Android 3.0 and 2.x before 2.3.4 trusts messages that are received from a PF_NETL

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from nvd@nist.gov

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.383410000 probability, percentile 0.972510000 (date 2026-05-04)

CISA KEV: Listed on 2022-09-08; due 2022-09-29; ransomware use Unknown

Problem Types: CWE-190 | n/a | CWE-190 CWE-190 Integer Overflow or Wraparound

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	ADP	DECLARED	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	7.2		AV:L/AC:L/Au:N/C:C/I:C/A:C

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:L/AC:L/Au:N/C:C/I:C/A:C

CISA Known Exploited Vulnerability

Vendor	Android
Product	Android OS
Name	Android OS Privilege Escalation Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://android.googlesource.com/platform/system/vold/+/c51920c82463b240e2be0430849837d6fdc5352e; https://nvd.nist.gov/vuln/detail/CVE-2011-1823

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Google	Android	All	All	All	All
Operating System	Google	Android	3.0	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
android.git.kernel.org	af854a3a
android.git.kernel.org	af854a3a
android.git.kernel.org	af854a3a
[App] [26.04.2011][v1.2] GingerBreak APK (root for GingerBread) | XDA Developers Forums	af854a3a
IBM X-Force Exchange	af854a3a
Google Patches GingerBreak Exploit, But Don't Worry - We Still Have Root (For Now)	af854a3a
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704
Android vold mPartMinors[] Signedness Issue « xorl %eax, %eax	af854a3a
GingerBreak (root for Gingerbread) app | Android Community	af854a3a
C skills: yummy yummy, GingerBreak!	af854a3a
CONFIRM:http://android.git.kernel.org/?p=platform/system/core.git;a=commit;h=b620a0b1c7ae486e979826200e8e441605b0a5d6	MITRE
CONFIRM:http://android.git.kernel.org/?p=platform/system/netd.git;a=commit;h=79b579c92afc08ab12c0a5788d61f2dd2934836f	MITRE
CONFIRM:http://android.git.kernel.org/?p=platform/system/vold.git;a=commit;h=c51920c82463b240e2be0430849837d6fdc5352e	MITRE
CVE Program record	CVE.OR
NVD vulnerability detail	NVD
CISA Known Exploited Vulnerabilities catalog	CISA

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
ADP	2022-09-08T00:00:00.000Z	CVE-2011-1823 added to CISA KEV

Legacy QID Mappings

610551 Google Android 2.x and 3.x Numeric Errors Vulnerability