CVE-2016-6789

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

Summary

CVE	CVE-2016-6789
State	PUBLISHED
Assigner	google_android
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-01-12 15:59:01 UTC
Updated	2026-05-06 22:30:45 UTC
Description	An elevation of privilege vulnerability in the NVIDIA libomx library (libnvomx) could enable a local malicious application to ex

Risk And Classification

Primary CVSS: v3.0 7.8 HIGH from nvd@nist.gov

CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

EPSS: 0.001470000 probability, percentile 0.347240000 (date 2026-05-10)

Problem Types: CWE-284 | Elevation of privilege

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	7.8	HIGH	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	9.3		AV:N/AC:M/Au:N/C:C/I:C/A:C

CVSS v3.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	3.18	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Google Inc.	Android	affected Kernel-3.18	Not specified

References

Reference	Source
Google Pixel C NVIDIA libomx Library Multiple Local Privilege Escalation Vulnerabilities	af854a3a-21
Security Bulletin: NVIDIA Tegra Jetson L4T contains multiple vulnerabilities; updates for “BlueBorne” and “Dnsmasq”. | NVIDIA	af854a3a-21
Android Security Bulletin—December 2016 | Android Open Source Project	af854a3a-21
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy OID mappings associated with this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**