CVE-2014-8002

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

Summary

CVE	CVE-2014-8002
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-11-25 17:59:01 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Use-after-free vulnerability in decode_slice.cpp in Cisco OpenH264 1.2.0 and earlier allows remote attackers to execute arb

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

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

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Openh264	All	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source	L
Cisco OpenH264 Media Processing Use-After-Free Vulnerability	af854a3a-2127-422b-91ae-364da2661108	t
stop early error for parse/recon MB by huili2 · Pull Request #1096 · cisco/openh264 · GitHub	af854a3a-2127-422b-91ae-364da2661108	g
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n

No vendor comments have been submitted for this CVE.

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