CVE-2007-4455

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

Summary

CVE	CVE-2007-4455
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-08-22 01:17:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	The SIP channel driver (chan_sip) in Asterisk Open Source 1.4.x before 1.4.11, AsteriskNOW before beta7, Asterisk Applia

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

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

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Asterisk	Asterisk	All	All	All	All

Application	Asterisk	Asterisknow	All	All	All	All
Application	Asterisk	Asterisk Appliance Developer Kit	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
Asterisk SIP Dialog History Processing Error Lets Remote Users Deny Service - SecurityTracker	af854a3a-2127-422b-91ae-364da2661108
Asterisk SIP Dialog History Resource Exhaustion Remote Denial of Service Vulnerability	af854a3a-2127-422b-91ae-364da2661108
Resource Exhaustion Vulnerability in Asterisk SIP channel driver - CXSecurity.com	af854a3a-2127-422b-91ae-364da2661108
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da2661108
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-364da2661108
Full Disclosure: AST-2007-020: Resource Exhaustion Vulnerability in Asterisk SIP channel driver	af854a3a-2127-422b-91ae-364da2661108
AST-2007-020	af854a3a-2127-422b-91ae-364da2661108
Asterisk SIP Channel Driver Dialog History Memory Exhaustion - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2661108
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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