CVE-2008-0095

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

Summary

CVE	CVE-2008-0095
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-01-08 02:46:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	The SIP channel driver in Asterisk Open Source 1.4.x before 1.4.17, Business Edition before C.1.0-beta8, AsteriskNOW be

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: CWE-399 | 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	Asterisknow	All	All	All	All

Application	Asterisk	Asterisk Appliance Developer Kit	All	All	All	All
Application	Asterisk	Asterisk Business Edition	All	All	All	All
Application	Asterisk	Open Source	All	All	All	All
Application	Asterisk	S800i	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
[SECURITY] Fedora 7 Update: asterisk-1.4.17-1.fc7	af854a3a-212
IBM X-Force Exchange	af854a3a-212
Asterisk "BYE/Also" Denial of Service Vulnerability - Secunia Advisories - Vulnerability Intelligence - Secunia.com	af854a3a-212
0011637: Also Header on BYE will Crash Asterisk - Digium Issue Tracker	af854a3a-212
[SECURITY] Fedora 8 Update: asterisk-1.4.17-1.fc8	af854a3a-212
AST-2008-001	af854a3a-212
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-212
Fedora update for asterisk - Advisories - Secunia	af854a3a-212
SecurityReason - Crash from transfer using BYE with Also header	af854a3a-212
Asterisk BYE Message Remote Denial of Service Vulnerability	af854a3a-212
SecurityFocus	af854a3a-212
SecurityTracker.com Archives - Asterisk SIP Channel Driver Can Be Crashed By Remote Users With 'BYE with Also' Method	af854a3a-212
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.

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