CVE-2008-1333

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

Summary

CVE	CVE-2008-1333
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-03-20 00:44:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Format string vulnerability in Asterisk Open Source 1.6.x before 1.6.0-beta6 might allow remote attackers to execute arbitra

Risk And Classification

Primary CVSS: v2.0 5.8 from nvd@nist.gov

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

Problem Types: CWE-134 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Asterisk	Open Source	1.6.0_beta1	All	All	All

Application	Asterisk	Open Source	1.6.0_beta2	All	All	All
Application	Asterisk	Open Source	1.6.0_beta3	All	All	All
Application	Asterisk	Open Source	1.6.0_beta4	All	All	All
Application	Asterisk	Open Source	1.6.0_beta5	All	All	All

Vendor Declared Affected Products

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

References

Reference	Sou
Asterisk Logger and Manager Format String Vulnerabilities	af85
Debian update for asterisk - Advisories - Secunia	af85
Asterisk :: The Open Source PBX & Telephony Platform | (Critical Updates) Asterisk 1.2.27, 1.4.18.1, 1.4.19-rc3, 1.6.0-beta6 Released	af85
Asterisk Format String Bug in Logger and Manager Lets Remote Users Deny Service - SecurityTracker	af85
IBM X-Force Exchange	af85
AST-2008-004	af85
Asterisk Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com	af85
SecurityFocus	af85
Debian -- Security Information -- DSA-1525-1 asterisk	af85
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af85
CVE Program record	CVE
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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