



CVE-2014-8412

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2014-8412
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-11-24 15:59:04 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The (1) VoIP channel drivers, (2) DUNDi, and (3) Asterisk Manager Interface (AMI) in Asterisk Open Source 1.8.x before 1.8.10.0 allow an attacker to execute arbitrary code via a crafted SIP message.

Risk And Classification

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

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

Problem Types: CWE-264 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

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

Application	Digium	Certified Asterisk	1.8.28	cert1	All	All
Application	Digium	Certified Asterisk	1.8.28	cert2	All	All
Application	Digium	Certified Asterisk	1.8.28.0	All	All	All
Application	Digium	Certified Asterisk	11.6	cert1	All	All
Application	Digium	Certified Asterisk	11.6	cert2	All	All
Application	Digium	Certified Asterisk	11.6	cert3	All	All
Application	Digium	Certified Asterisk	11.6	cert4	All	All
Application	Digium	Certified Asterisk	11.6	cert5	All	All
Application	Digium	Certified Asterisk	11.6	cert6	All	All
Application	Digium	Certified Asterisk	11.6	cert7	All	All
Application	Digium	Certified Asterisk	11.6.0	All	All	All

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

References			
Reference	Source	Link	Tags
AST-2014-012	af854a3a-2127-422b-91ae-364da2661108	downloads.asterisk.org	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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