CVE-2017-9359

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

Summary

CVE	CVE-2017-9359
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-06-02 05:29:00 UTC
Updated	2025-04-20 01:37:25 UTC
Description	The multi-part body parser in PJSIP, as used in Asterisk Open Source 13.x before 13.15.1 and 14.x before 14.4.1, Certified

Risk And Classification

Primary CVSS: v3.0 7.5 HIGH from nvd@nist.gov

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Problem Types: CWE-125 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
2.0	nvd@nist.gov	Primary	5		AV:N/AC:L/Au:N/C:N/I:N/A:P

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

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	Digium	Certified Asterisk	13.13.0	All	All	All
Application	Digium	Certified Asterisk	13.13.0	cert1	All	All
Application	Digium	Certified Asterisk	13.13.0	cert1-rc1	All	All
Application	Digium	Certified Asterisk	13.13.0	cert1-rc2	All	All
Application	Digium	Certified Asterisk	13.13.0	cert1-rc3	All	All
Application	Digium	Certified Asterisk	13.13.0	cert1-rc4	All	All
Application	Digium	Certified Asterisk	13.13.0	cert2	All	All
Application	Digium	Certified Asterisk	13.13.0	cert3	All	All
Application	Digium	Certified Asterisk	13.13.0	rc1	All	All
Application	Digium	Certified Asterisk	13.13.0	rc2	All	All
Application	Digium	Open Source	13.0.0	All	All	All
Application	Digium	Open Source	13.1.0	All	All	All
Application	Digium	Open Source	13.1.0	rc1	All	All
Application	Digium	Open Source	13.1.0	rc2	All	All
Application	Digium	Open Source	13.10.0	rc1	All	All
Application	Digium	Open Source	13.11.0	rc1	All	All
Application	Digium	Open Source	13.12.0	All	All	All

Application	Digium	Open Source	13.12.0	rc1	All	All
Application	Digium	Open Source	13.12.1	All	All	All
Application	Digium	Open Source	13.12.2	All	All	All
Application	Digium	Open Source	13.13.0	rc1	All	All
Application	Digium	Open Source	13.14.0	rc1	All	All
Application	Digium	Open Source	13.15.0	rc1	All	All
Application	Digium	Open Source	13.2.0	All	All	All
Application	Digium	Open Source	13.2.0	rc1	All	All
Application	Digium	Open Source	13.3.0	rc1	All	All
Application	Digium	Open Source	13.4.0	All	All	All
Application	Digium	Open Source	13.4.0	rc1	All	All
Application	Digium	Open Source	13.5.0	All	All	All
Application	Digium	Open Source	13.5.0	rc1	All	All
Application	Digium	Open Source	13.6.0	rc1	All	All
Application	Digium	Open Source	13.7.0	All	All	All
Application	Digium	Open Source	13.7.0	rc1	All	All
Application	Digium	Open Source	13.8.0	All	All	All
Application	Digium	Open Source	13.8.0	rc1	All	All
Application	Digium	Open Source	13.8.1	All	All	All
Application	Digium	Open Source	13.8.2	All	All	All
Application	Digium	Open Source	13.9.0	All	All	All
Application	Digium	Open Source	13.9.0	rc1	All	All
Application	Digium	Open Source	14.2.0	All	All	All
Application	Digium	Open Source	14.2.0	rc1	All	All
Application	Digium	Open Source	14.2.0	rc2	All	All

Vendor Declared Affected Products

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

References

Reference	Source
[ASTERISK-26939] Out of bound memory access in PJSIP multipart parser crashes Asterisk - Digium/Asterisk JIRA	af854a3a-2127-422b-9
Multiple Asterisk Products Denial of Service Vulnerability	af854a3a-2127-422b-9
downloads.asterisk.org/pub/security/AST-2017-003.txt	af854a3a-2127-422b-9
Debian -- Security Information -- DSA-3933-1 pjproject	af854a3a-2127-422b-9

#863902 - pjproject: AST-2017-003: Crash in PJSIP multi-part body parser - Debian Bug report logs	af854a3a-2127-422b-9
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.