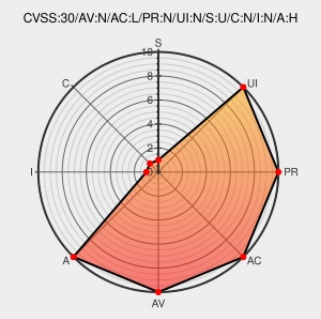
CVE-2016-9937

Published on: 12/12/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:16 PM UTC

CVE-2016-9937

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Asterisk from Digium contain the following vulnerability:

An issue was discovered in Asterisk Open Source 13.12.x and 13.13.x before 13.13.1 and 14.x before 14.2.1. If an SDP offer or answer is received with the Opus codec and with the format parameters separated using a space the code responsible for parsing will recursively call itself until it crashes. This occurs as the code does not properly handle spaces separating the parameters. This does NOT require the endpoint to have Opus configured in Asterisk. This also does not require the endpoint to be authenticated. If guest is enabled for chan_sip or anonymous in chan_pjsip an SDP offer or answer is still processed and the crash occurs.

CVE-2016-9937 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
	Patch Vendor Advisory downloads.asterisk.org text/x-diff	CONFIRM downloads.asterisk.org/pub/security/AST-2016-008-14.diff
[ASTERISK-26579] codec_opus: Recursiveness when parsing fmtp line - Digium/Asterisk JIRA	Patch Vendor Advisory issues.asterisk.org text/html	CONFIRM issues.asterisk.org/jira/browse/ASTERISK-26579
Asterisk Open Source AST-2016-008 Denial of Service Vulnerability	Third Party Advisory VDB Entry cve.report (archive) text/html	BID 94792
	Patch Vendor Advisory downloads.asterisk.org text/x-diff	CONFIRM downloads.asterisk.org/pub/security/AST-2016-008-13.diff
Asterisk Message Parsing Flaw in sdp_fmtp_get() Lets Remote Users Cause the Target Service to Crash - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1037407
AST-2016-008	Patch Vendor Advisory downloads.asterisk.org text/html	CONFIRM downloads.asterisk.org/pub/security/AST-2016-008.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Digium	Asterisk	13.12	All	All	All
Application	Digium	Asterisk	13.13	All	All	All
Application	Digium	Asterisk	14.0	All	All	All
Application	Digium	Asterisk	14.01	All	All	All
Application	Digium	Asterisk	14.02	All	All	All
Application	Digium	Asterisk	14.1	All	All	All
Application	Digium	Asterisk	14.1.1	All	All	All
Application	Digium	Asterisk	14.1.2	All	All	All
Application	Digium	Asterisk	14.2	All	All	All
Application	Digium	Asterisk	13.12	All	All	All
Application	Digium	Asterisk	13.13	All	All	All
Application	Digium	Asterisk	14.0	All	All	All

Application	Digium	Asterisk	14.01	All	All	All
Application	Digium	Asterisk	14.02	All	All	All
Application	Digium	Asterisk	14.1	All	All	All
Application	Digium	Asterisk	14.1.1	All	All	All
Application	Digium	Asterisk	14.1.2	All	All	All
Application	Digium	Asterisk	14.2	All	All	All

cpe:2.3:a:digium:asterisk:13.12:*:*:*:*:*:*:*:

cpe:2.3:a:digium:asterisk:13.13:*:*:*:*:*:*:*:

cpe:2.3:a:digium:asterisk:14.0:*:*:*:*:*:*:*:

cpe:2.3:a:digium:asterisk:14.01:*:*:*:*:*:*:*:

cpe:2.3:a:digium:asterisk:14.02:*:*:*:*:*:*:*:

cpe:2.3:a:digium:asterisk:14.1:*:*:*:*:*:*:*:

cpe:2.3:a:digium:asterisk:14.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:digium:asterisk:14.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:digium:asterisk:14.2:*:*:*:*:*:*:*:

cpe:2.3:a:digium:asterisk:13.12:*:*:*:*:*:*:*:

cpe:2.3:a:digium:asterisk:13.13:*:*:*:*:*:*:*:

cpe:2.3:a:digium:asterisk:14.0:*:*:*:*:*:*:*:

cpe:2.3:a:digium:asterisk:14.01:*:*:*:*:*:*:*:

cpe:2.3:a:digium:asterisk:14.02:*:*:*:*:*:*:*:

cpe:2.3:a:digium:asterisk:14.1:*:*:*:*:*:*:*:

cpe:2.3:a:digium:asterisk:14.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:digium:asterisk:14.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:digium:asterisk:14.2:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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