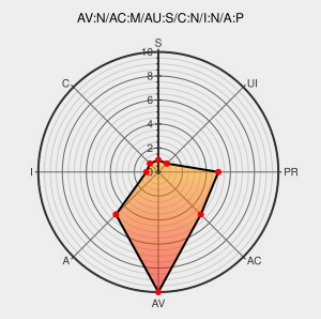
CVE-2014-2289

Published on: 04/18/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:58 PM UTC

CVE-2014-2289

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



Certain versions of Asterisk from Digium contain the following vulnerability:

res/res_pjsip_exten_state.c in the PJSIP channel driver in Asterisk Open Source 12.x before 12.1.0 allows remote authenticated users to cause a denial of service (crash) via a SUBSCRIBE request without any Accept headers, which triggers an invalid pointer dereference.

CVE-2014-2289 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 3.5 - LOW

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

CVE References

Description	Tags	Link
[SECURITY] Fedora 19 Update: asterisk-11.8.1-1.fc19	lists.fedoraproject.org, text/html	FEDORA FEDORA-2014-3779
AST-2014-004	Patch, Vendor Advisory, downloads.asterisk.org, text/html	CONFIRM downloads.asterisk.org/pub/security/AST-2014-004.html
	Patch, downloads.asterisk.org, text/x-diff	MISC downloads.asterisk.org/pub/security/AST-2014-004-12.diff
[SECURITY] Fedora 20 Update: asterisk-11.8.1-1.fc20	lists.fedoraproject.org, text/html	FEDORA FEDORA-2014-3762
[ASTERISK-23139] Security: Remote crash in res_pjsip_exten_state - Digium/Asterisk JIRA	issues.asterisk.org, text/html	CONFIRM issues.asterisk.org/jira/browse/ASTERISK-

23139

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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	12.0.0	All	All	All
Application	Digium	Asterisk	12.1.0	rc1	All	All
Application	Digium	Asterisk	12.1.0	rc2	All	All
Application	Digium	Asterisk	12.1.0	rc3	All	All
Application	Digium	Asterisk	12.0.0	All	All	All
Application	Digium	Asterisk	12.1.0	rc1	All	All
Application	Digium	Asterisk	12.1.0	rc2	All	All
Application	Digium	Asterisk	12.1.0	rc3	All	All

cpe:2.3:a:digium:asterisk:12.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:digium:asterisk:12.1.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:digium:asterisk:12.1.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:digium:asterisk:12.1.0:rc3:*:*:*:*:*:*:

cpe:2.3:a:digium:asterisk:12.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:digium:asterisk:12.1.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:digium:asterisk:12.1.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:digium:asterisk:12.1.0:rc3:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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