



CVE-2014-8417

Published on: 11/24/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:51 PM UTC

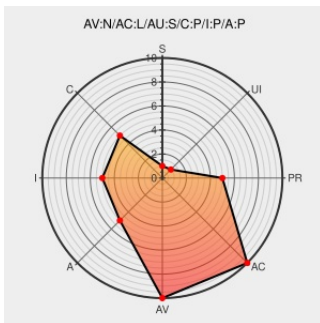
CVE-2014-8417

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Asterisk](#) from [Digium](#) contain the following vulnerability:

ConfBridge in Asterisk 11.x before 11.14.1, 12.x before 12.7.1, and 13.x before 13.0.1 and Certified Asterisk 11.6 before 11.6-cert8 allows remote authenticated users to (1) gain privileges via vectors related to an external protocol to the CONFBRIDGE dialplan function or (2) execute arbitrary system commands via a crafted

ConfbridgeStartRecord AMI action.

CVE-2014-8417 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **6.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
AST-2014-017	Vendor Advisory downloads.asterisk.org text/html	CONFIRM downloads.asterisk.org/pub/security/AST-2014-017.html

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	All	All	All	All
Application	Digium	Asterisk	All	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
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
cpe:2.3:a:digium:asterisk:*****:.*:						
cpe:2.3:a:digium:asterisk:*****:.*:						
cpe:2.3:a:digium:certified_asterisk:11.6:cert1:*****:.*:						
cpe:2.3:a:digium:certified_asterisk:11.6:cert2:*****:.*:						
cpe:2.3:a:digium:certified_asterisk:11.6:cert3:*****:.*:						
cpe:2.3:a:digium:certified_asterisk:11.6:cert4:*****:.*:						
cpe:2.3:a:digium:certified_asterisk:11.6:cert5:*****:.*:						
cpe:2.3:a:digium:certified_asterisk:11.6:cert6:*****:.*:						
cpe:2.3:a:digium:certified_asterisk:11.6:cert7:*****:.*:						
cpe:2.3:a:digium:certified_asterisk:11.6.0:-:*****:.*:						
cpe:2.3:a:digium:certified_asterisk:11.6:cert1:*****:.*:						
cpe:2.3:a:digium:certified_asterisk:11.6:cert2:*****:.*:						

cpe:2.3:a:digium:certified_asterisk:11.6:cert3:*:*:*:*:*:
cpe:2.3:a:digium:certified_asterisk:11.6:cert4:*:*:*:*:*:
cpe:2.3:a:digium:certified_asterisk:11.6:cert5:*:*:*:*:*:
cpe:2.3:a:digium:certified_asterisk:11.6:cert6:*:*:*:*:*:
cpe:2.3:a:digium:certified_asterisk:11.6:cert7:*:*:*:*:*:
cpe:2.3:a:digium:certified_asterisk:11.6.0:-:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)