

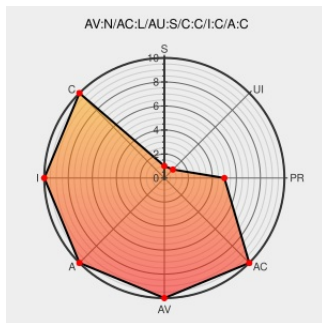


CVE-2014-8418

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

Last Modified on: 03/23/2021 11:25:52 PM UTC

CVE-2014-8418

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

The DB dialplan function in Asterisk Open Source 1.8.x before 1.8.32, 11.x before 11.1.4.1, 12.x before 12.7.1, and 13.x before 13.0.1 and Certified Asterisk 1.8 before 1.8.28-cert8 and 11.6 before 11.6-cert8 allows remote authenticated users to gain privileges via a call from an external protocol, as demonstrated by the AMI protocol.

CVE-2014-8418 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **9 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

SINGLE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

AST-2014-018

[Vendor Advisory](#)
[downloads.asterisk.org](#)
[text/html](#)

[CONFIRM downloads.asterisk.org/pub/security/AST-2014-018.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	Asterisk	All	All	All	All
Application	Digium	Certified Asterisk	1.8.28	All	All	All
Application	Digium	Certified Asterisk	1.8.28	cert1	All	All
Application	Digium	Certified Asterisk	1.8.28	cert1-rc1	All	All
Application	Digium	Certified Asterisk	1.8.28	cert2	All	All
Application	Digium	Certified Asterisk	1.8.28	cert2	All	All
Application	Digium	Certified Asterisk	1.8.28	cert3	All	All
Application	Digium	Certified Asterisk	1.8.28	cert4	All	All
Application	Digium	Certified Asterisk	1.8.28	cert5	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	1.8.28	All	All	All
Application	Digium	Certified Asterisk	1.8.28	cert1	All	All
Application	Digium	Certified Asterisk	1.8.28	cert1-rc1	All	All
Application	Digium	Certified Asterisk	1.8.28	cert2	All	All
Application	Digium	Certified Asterisk	1.8.28	cert2	All	All
Application	Digium	Certified Asterisk	1.8.28	cert3	All	All
Application	Digium	Certified Asterisk	1.8.28	cert4	All	All
Application	Digium	Certified Asterisk	1.8.28	cert5	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:asterisk:*.*.*.*.*.*.*.*:						
cpe:2.3:a:digium:certified_asterisk:1.8.28:*.*.*.*.*.*.*.*:						
cpe:2.3:a:digium:certified_asterisk:1.8.28:cert1:*.*.*.*.*.*.*.*:						
cpe:2.3:a:digium:certified_asterisk:1.8.28:cert1-rc1:*.*.*.*.*.*.*.*:						
cpe:2.3:a:digium:certified_asterisk:1.8.28:cert2:*.*.*.*.*.*.*.*:						
cpe:2.3:a:digium:certified_asterisk:1.8.28:cert2:*.*.*.*.*.*.*.*:						
cpe:2.3:a:digium:certified_asterisk:1.8.28:cert3:*.*.*.*.*.*.*.*:						
cpe:2.3:a:digium:certified_asterisk:1.8.28:cert4:*.*.*.*.*.*.*.*:						
cpe:2.3:a:digium:certified_asterisk:1.8.28:cert5:*.*.*.*.*.*.*.*:						
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:1.8.28:*.*.*.*.*.*.*.*:						
cpe:2.3:a:digium:certified_asterisk:1.8.28:cert1:*.*.*.*.*.*.*.*:						
cpe:2.3:a:digium:certified_asterisk:1.8.28:cert1-rc1:*.*.*.*.*.*.*.*:						
cpe:2.3:a:digium:certified_asterisk:1.8.28:cert2:*.*.*.*.*.*.*.*:						
cpe:2.3:a:digium:certified_asterisk:1.8.28:cert2:*.*.*.*.*.*.*.*:						
cpe:2.3:a:digium:certified_asterisk:1.8.28:cert3:*.*.*.*.*.*.*.*:						
cpe:2.3:a:digium:certified_asterisk:1.8.28:cert4:*.*.*.*.*.*.*.*:						
cpe:2.3:a:digium:certified_asterisk:1.8.28:cert5:*.*.*.*.*.*.*.*:						

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 →