



CVE-2011-2665

Published on: 07/06/2011 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:22 PM UTC

CVE-2011-2665

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

reqresp_parser.c in the SIP channel driver in Asterisk Open Source 1.8.x before 1.8.4.3 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via a SIP packet with a Contact header that lacks a < (less than) character.

CVE-2011-2665 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

[SECURITY] Fedora 14 Update: asterisk-1.6.2.19-1.fc14

[lists.fedoraproject.org](#)
[text/html](#)

[FEDORA FEDORA-2011-8914](#)

AST-2011-009

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

[CONFIRM downloads.asterisk.org/pub/security/AST-2011-009.html](#)

[Patch](#)
[downloads.asterisk.org](#)
[text/x-diff](#)

[CONFIRM downloads.asterisk.org/pub/security/AST-2011-009-1.8.diff](#)

Asterisk Multiple Denial of Service Vulnerabilities - Secunia.com

[Vendor Advisory](#)
[web.archive.org](#)
[text/html](#)

[SECUNIA 45048](#)

Debian update for asterisk - Secunia.com

[web.archive.org](#)
[text/html](#)

[SECUNIA 45201](#)

Fedora update for asterisk - Secunia.com

web.archive.org
text/html

X SECUNIA 45239

Debian -- Security Information -- DSA-2276-1 asterisk

www.debian.org
Depreciated Link
text/html

DEBIAN DSA-2276

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	1.8.0	All	All	All
Application	Digium	Asterisk	1.8.0	beta1	All	All
Application	Digium	Asterisk	1.8.0	beta2	All	All
Application	Digium	Asterisk	1.8.0	beta3	All	All
Application	Digium	Asterisk	1.8.0	beta4	All	All
Application	Digium	Asterisk	1.8.0	beta5	All	All
Application	Digium	Asterisk	1.8.0	rc2	All	All
Application	Digium	Asterisk	1.8.0	rc3	All	All
Application	Digium	Asterisk	1.8.0	rc4	All	All
Application	Digium	Asterisk	1.8.0	rc5	All	All
Application	Digium	Asterisk	1.8.1	All	All	All
Application	Digium	Asterisk	1.8.1	rc1	All	All
Application	Digium	Asterisk	1.8.1.1	All	All	All
Application	Digium	Asterisk	1.8.1.2	All	All	All
Application	Digium	Asterisk	1.8.2	All	All	All
Application	Digium	Asterisk	1.8.2.1	All	All	All
Application	Digium	Asterisk	1.8.2.2	All	All	All
Application	Digium	Asterisk	1.8.2.3	All	All	All
Application	Digium	Asterisk	1.8.2.4	All	All	All
Application	Digium	Asterisk	1.8.3	All	All	All
Application	Digium	Asterisk	1.8.3	rc1	All	All
Application	Digium	Asterisk	1.8.3	rc2	All	All
Application	Digium	Asterisk	1.8.3	rc3	All	All
Application	Digium	Asterisk	1.8.3.1	All	All	All

Application	Engine	Protocol	Version	Arch	OS	Platform
Application	Digium	Asterisk	1.8.3.2	All	All	All
Application	Digium	Asterisk	1.8.3.3	All	All	All
Application	Digium	Asterisk	1.8.4	All	All	All
Application	Digium	Asterisk	1.8.4	rc1	All	All
Application	Digium	Asterisk	1.8.4	rc2	All	All
Application	Digium	Asterisk	1.8.4	rc3	All	All
Application	Digium	Asterisk	1.8.4.1	All	All	All
Application	Digium	Asterisk	1.8.4.2	All	All	All
Application	Digium	Asterisk	1.8.0	All	All	All
Application	Digium	Asterisk	1.8.0	beta1	All	All
Application	Digium	Asterisk	1.8.0	beta2	All	All
Application	Digium	Asterisk	1.8.0	beta3	All	All
Application	Digium	Asterisk	1.8.0	beta4	All	All
Application	Digium	Asterisk	1.8.0	beta5	All	All
Application	Digium	Asterisk	1.8.0	rc2	All	All
Application	Digium	Asterisk	1.8.0	rc3	All	All
Application	Digium	Asterisk	1.8.0	rc4	All	All
Application	Digium	Asterisk	1.8.0	rc5	All	All
Application	Digium	Asterisk	1.8.1	All	All	All
Application	Digium	Asterisk	1.8.1	rc1	All	All
Application	Digium	Asterisk	1.8.1.1	All	All	All
Application	Digium	Asterisk	1.8.1.2	All	All	All
Application	Digium	Asterisk	1.8.2	All	All	All
Application	Digium	Asterisk	1.8.2.1	All	All	All
Application	Digium	Asterisk	1.8.2.2	All	All	All
Application	Digium	Asterisk	1.8.2.3	All	All	All
Application	Digium	Asterisk	1.8.2.4	All	All	All
Application	Digium	Asterisk	1.8.3	All	All	All
Application	Digium	Asterisk	1.8.3	rc1	All	All
Application	Digium	Asterisk	1.8.3	rc2	All	All
Application	Digium	Asterisk	1.8.3	rc3	All	All
Application	Digium	Asterisk	1.8.3.1	All	All	All
Application	Digium	Asterisk	1.8.3.2	All	All	All
Application	Digium	Asterisk	1.8.3.3	All	All	All
Application	Digium	Asterisk	1.8.4	All	All	All

Application	Digium	Asterisk	1.8.4	rc1	All	All
Application	Digium	Asterisk	1.8.4	rc2	All	All
Application	Digium	Asterisk	1.8.4	rc3	All	All
Application	Digium	Asterisk	1.8.4.1	All	All	All
Application	Digium	Asterisk	1.8.4.2	All	All	All
cpe:2.3:a:digium:asterisk:1.8.0:*****.**:						
cpe:2.3:a:digium:asterisk:1.8.0:beta1:*****.**:						
cpe:2.3:a:digium:asterisk:1.8.0:beta2:*****.**:						
cpe:2.3:a:digium:asterisk:1.8.0:beta3:*****.**:						
cpe:2.3:a:digium:asterisk:1.8.0:beta4:*****.**:						
cpe:2.3:a:digium:asterisk:1.8.0:beta5:*****.**:						
cpe:2.3:a:digium:asterisk:1.8.0:rc2:*****.**:						
cpe:2.3:a:digium:asterisk:1.8.0:rc3:*****.**:						
cpe:2.3:a:digium:asterisk:1.8.0:rc4:*****.**:						
cpe:2.3:a:digium:asterisk:1.8.0:rc5:*****.**:						
cpe:2.3:a:digium:asterisk:1.8.1:*****.**:						
cpe:2.3:a:digium:asterisk:1.8.1:rc1:*****.**:						
cpe:2.3:a:digium:asterisk:1.8.1.1:*****.**:						
cpe:2.3:a:digium:asterisk:1.8.1.2:*****.**:						
cpe:2.3:a:digium:asterisk:1.8.2:*****.**:						
cpe:2.3:a:digium:asterisk:1.8.2.1:*****.**:						
cpe:2.3:a:digium:asterisk:1.8.2.2:*****.**:						
cpe:2.3:a:digium:asterisk:1.8.2.3:*****.**:						
cpe:2.3:a:digium:asterisk:1.8.2.4:*****.**:						
cpe:2.3:a:digium:asterisk:1.8.3:*****.**:						
cpe:2.3:a:digium:asterisk:1.8.3:rc1:*****.**:						
cpe:2.3:a:digium:asterisk:1.8.3:rc2:*****.**:						
cpe:2.3:a:digium:asterisk:1.8.3:rc3:*****.**:						
cpe:2.3:a:digium:asterisk:1.8.3.1:*****.**:						

cpe:2.3:a:digium:asterisk:1.8.3.2:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:digium:asterisk:1.8.3.3:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:digium:asterisk:1.8.4:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:digium:asterisk:1.8.4:rc1:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:digium:asterisk:1.8.4:rc2:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:digium:asterisk:1.8.4:rc3:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:digium:asterisk:1.8.4.1:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:digium:asterisk:1.8.4.2:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:digium:asterisk:1.8.0:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:digium:asterisk:1.8.0:beta1:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:digium:asterisk:1.8.0:beta2:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:digium:asterisk:1.8.0:beta3:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:digium:asterisk:1.8.0:beta4:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:digium:asterisk:1.8.0:beta5:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:digium:asterisk:1.8.0:rc2:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:digium:asterisk:1.8.0:rc3:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:digium:asterisk:1.8.0:rc4:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:digium:asterisk:1.8.0:rc5:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:digium:asterisk:1.8.1:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:digium:asterisk:1.8.1:rc1:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:digium:asterisk:1.8.1.1:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:digium:asterisk:1.8.1.2:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:digium:asterisk:1.8.2:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:digium:asterisk:1.8.2.1:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:digium:asterisk:1.8.2.2:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:digium:asterisk:1.8.2.3:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:digium:asterisk:1.8.2.4:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:digium:asterisk:1.8.3:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:digium:asterisk:1.8.3:rc1:~::~~::~~::~~::~~::~~::~~:::

cpe:2.3:a:digium:asterisk:1.8.3:rc2:~::~~::~~::~~::~~::~~::~::
cpe:2.3:a:digium:asterisk:1.8.3:rc3:~::~~::~~::~~::~~::~~::~::
cpe:2.3:a:digium:asterisk:1.8.3.1:~::~~::~~::~~::~~::~~::~::
cpe:2.3:a:digium:asterisk:1.8.3.2:~::~~::~~::~~::~~::~~::~::
cpe:2.3:a:digium:asterisk:1.8.3.3:~::~~::~~::~~::~~::~~::~::
cpe:2.3:a:digium:asterisk:1.8.4:~::~~::~~::~~::~~::~~::~::
cpe:2.3:a:digium:asterisk:1.8.4:rc1:~::~~::~~::~~::~~::~~::~::
cpe:2.3:a:digium:asterisk:1.8.4:rc2:~::~~::~~::~~::~~::~~::~::
cpe:2.3:a:digium:asterisk:1.8.4:rc3:~::~~::~~::~~::~~::~~::~::
cpe:2.3:a:digium:asterisk:1.8.4.1:~::~~::~~::~~::~~::~~::~::
cpe:2.3:a:digium:asterisk:1.8.4.2:~::~~::~~::~~::~~::~~::~::

No vendor comments have been submitted for this CVE