



CVE-2015-1558

Published on: 02/09/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:09 PM UTC

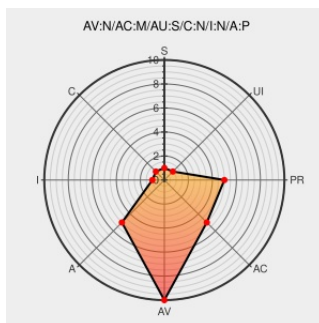
CVE-2015-1558

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

Asterisk Open Source 12.x before 12.8.1 and 13.x before 13.1.1, when using the PJSIP channel driver, does not properly reclaim RTP ports, which allows remote authenticated users to cause a denial of service (file descriptor consumption) via an SDP offer containing only incompatible codecs.

CVE-2015-1558 has been assigned by [M](#) 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

Asterisk File Descriptor Leak Lets Remote Authenticated Users Deny Service - SecurityTracker

www.securitytracker.com
text/html

[SECTRAK 1031661](#)

SecurityFocus

www.securityfocus.com
text/html

[BUGTRAQ 20150128 AST-2015-001: File descriptor leak when incompatible codecs are offered](#)

AST-2015-001

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

[CONFIRM](#)
downloads.asterisk.org/pub/security/AST-2015-001.html

Full Disclosure: AST-2015-001: File descriptor leak when incompatible codecs are offered

seclists.org
text/html

[FULLDISC 20150128 AST-2015-001: File descriptor leak when incompatible codecs are offered](#)

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	-	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	12.1.1	All	All	All
Application	Digium	Asterisk	12.2.0	All	All	All
Application	Digium	Asterisk	12.2.0	rc1	All	All
Application	Digium	Asterisk	12.2.0	rc2	All	All
Application	Digium	Asterisk	12.2.0	rc3	All	All
Application	Digium	Asterisk	12.3.0	All	All	All
Application	Digium	Asterisk	12.3.0	rc1	All	All
Application	Digium	Asterisk	12.3.0	rc2	All	All
Application	Digium	Asterisk	12.3.1	All	All	All
Application	Digium	Asterisk	12.3.2	All	All	All
Application	Digium	Asterisk	12.4.0	All	All	All
Application	Digium	Asterisk	12.4.0	rc1	All	All
Application	Digium	Asterisk	12.5.0	All	All	All
Application	Digium	Asterisk	12.5.0	rc1	All	All
Application	Digium	Asterisk	12.6.0	All	All	All
Application	Digium	Asterisk	12.6.0	rc1	All	All
Application	Digium	Asterisk	12.7.0	All	All	All
Application	Digium	Asterisk	12.7.0	rc1	All	All
Application	Digium	Asterisk	12.7.0	rc2	All	All
Application	Digium	Asterisk	12.8.0	All	All	All
Application	Digium	Asterisk	12.8.0	rc1	All	All
Application	Digium	Asterisk	12.8.0	rc2	All	All
Application	Digium	Asterisk	12.8.1	All	All	All

Application	Digium	Asterisk	13.0.0	All	All	All
Application	Digium	Asterisk	13.1.0	All	All	All
Application	Digium	Asterisk	13.1.0	rc1	All	All
Application	Digium	Asterisk	13.1.0	rc2	All	All
Application	Digium	Asterisk	13.2.0	All	All	All
Application	Digium	Asterisk	13.2.0	rc1	All	All
Application	Digium	Asterisk	12.0.0	All	All	All
Application	Digium	Asterisk	12.1.0	-	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	12.1.1	All	All	All
Application	Digium	Asterisk	12.2.0	All	All	All
Application	Digium	Asterisk	12.2.0	rc1	All	All
Application	Digium	Asterisk	12.2.0	rc2	All	All
Application	Digium	Asterisk	12.2.0	rc3	All	All
Application	Digium	Asterisk	12.3.0	All	All	All
Application	Digium	Asterisk	12.3.0	rc1	All	All
Application	Digium	Asterisk	12.3.0	rc2	All	All
Application	Digium	Asterisk	12.3.1	All	All	All
Application	Digium	Asterisk	12.3.2	All	All	All
Application	Digium	Asterisk	12.4.0	All	All	All
Application	Digium	Asterisk	12.4.0	rc1	All	All
Application	Digium	Asterisk	12.5.0	All	All	All
Application	Digium	Asterisk	12.5.0	rc1	All	All
Application	Digium	Asterisk	12.6.0	All	All	All
Application	Digium	Asterisk	12.6.0	rc1	All	All
Application	Digium	Asterisk	12.7.0	All	All	All
Application	Digium	Asterisk	12.7.0	rc1	All	All
Application	Digium	Asterisk	12.7.0	rc2	All	All
Application	Digium	Asterisk	12.8.0	All	All	All
Application	Digium	Asterisk	12.8.0	rc1	All	All
Application	Digium	Asterisk	12.8.0	rc2	All	All
Application	Digium	Asterisk	12.8.1	All	All	All
Application	Digium	Asterisk	13.0.0	All	All	All

Application	Digium	Asterisk	13.1.0	All	All	All
Application	Digium	Asterisk	13.1.0	rc1	All	All
Application	Digium	Asterisk	13.1.0	rc2	All	All
Application	Digium	Asterisk	13.2.0	All	All	All
Application	Digium	Asterisk	13.2.0	rc1	All	All
cpe:2.3:a:digium:asterisk:12.0.0:*:*:*:*:*:						
cpe:2.3:a:digium:asterisk:12.1.0:-:*:*:*:*:						
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:12.1.1:*:*:*:*:						
cpe:2.3:a:digium:asterisk:12.2.0:*:*:*:*:						
cpe:2.3:a:digium:asterisk:12.2.0:rc1:*:*:*:*:						
cpe:2.3:a:digium:asterisk:12.2.0:rc2:*:*:*:*:						
cpe:2.3:a:digium:asterisk:12.2.0:rc3:*:*:*:*:						
cpe:2.3:a:digium:asterisk:12.3.0:*:*:*:*:						
cpe:2.3:a:digium:asterisk:12.3.0:rc1:*:*:*:*:						
cpe:2.3:a:digium:asterisk:12.3.0:rc2:*:*:*:*:						
cpe:2.3:a:digium:asterisk:12.3.1:*:*:*:*:						
cpe:2.3:a:digium:asterisk:12.3.2:*:*:*:*:						
cpe:2.3:a:digium:asterisk:12.4.0:*:*:*:*:						
cpe:2.3:a:digium:asterisk:12.4.0:rc1:*:*:*:*:						
cpe:2.3:a:digium:asterisk:12.5.0:*:*:*:*:						
cpe:2.3:a:digium:asterisk:12.5.0:rc1:*:*:*:*:						
cpe:2.3:a:digium:asterisk:12.6.0:*:*:*:*:						
cpe:2.3:a:digium:asterisk:12.6.0:rc1:*:*:*:*:						
cpe:2.3:a:digium:asterisk:12.7.0:*:*:.lts:*:*:						
cpe:2.3:a:digium:asterisk:12.7.0:rc1:*:*:*:*:						
cpe:2.3:a:digium:asterisk:12.7.0:rc2:*:*:*:*:						
cpe:2.3:a:digium:asterisk:12.8.0:*:*:*:*:						

cpe:2.3:a:digium:asterisk:12.8.0:rc1:~::~~::~~::~~::~~::~::
cpe:2.3:a:digium:asterisk:12.8.0:rc2:~::~~::~~::~~::~~::~::
cpe:2.3:a:digium:asterisk:12.8.1:~::~~::~~::~~::~~::~::
cpe:2.3:a:digium:asterisk:13.0.0:~::~~::~~::~~::~~::~::
cpe:2.3:a:digium:asterisk:13.1.0:~::~~::~~::~~::~~::~::
cpe:2.3:a:digium:asterisk:13.1.0:rc1:~::~~::~~::~~::~~::~::
cpe:2.3:a:digium:asterisk:13.1.0:rc2:~::~~::~~::~~::~~::~::
cpe:2.3:a:digium:asterisk:13.2.0:~::~~::~~::~~::~~::~::
cpe:2.3:a:digium:asterisk:13.2.0:rc1:~::~~::~~::~~::~~::~::
cpe:2.3:a:digium:asterisk:12.0.0:~::~~::~~::~~::~~::~::
cpe:2.3:a:digium:asterisk:12.1.0:~::~~::~~::~~::~~::~::
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:12.1.1:~::~~::~~::~~::~~::~::
cpe:2.3:a:digium:asterisk:12.2.0:~::~~::~~::~~::~~::~::
cpe:2.3:a:digium:asterisk:12.2.0:rc1:~::~~::~~::~~::~~::~::
cpe:2.3:a:digium:asterisk:12.2.0:rc2:~::~~::~~::~~::~~::~::
cpe:2.3:a:digium:asterisk:12.2.0:rc3:~::~~::~~::~~::~~::~::
cpe:2.3:a:digium:asterisk:12.3.0:~::~~::~~::~~::~~::~::
cpe:2.3:a:digium:asterisk:12.3.0:rc1:~::~~::~~::~~::~~::~::
cpe:2.3:a:digium:asterisk:12.3.0:rc2:~::~~::~~::~~::~~::~::
cpe:2.3:a:digium:asterisk:12.3.1:~::~~::~~::~~::~~::~::
cpe:2.3:a:digium:asterisk:12.3.2:~::~~::~~::~~::~~::~::
cpe:2.3:a:digium:asterisk:12.4.0:~::~~::~~::~~::~~::~::
cpe:2.3:a:digium:asterisk:12.4.0:rc1:~::~~::~~::~~::~~::~::
cpe:2.3:a:digium:asterisk:12.5.0:~::~~::~~::~~::~~::~::
cpe:2.3:a:digium:asterisk:12.5.0:rc1:~::~~::~~::~~::~~::~::

cpe:2.3:a:digium:asterisk:12.6.0:*:*:*:*:*:
cpe:2.3:a:digium:asterisk:12.6.0:rc1:*:*:*:*:*:
cpe:2.3:a:digium:asterisk:12.7.0:*:*:*:lts.*:*:
cpe:2.3:a:digium:asterisk:12.7.0:rc1:*:*:*:*:*:
cpe:2.3:a:digium:asterisk:12.7.0:rc2:*:*:*:*:*:
cpe:2.3:a:digium:asterisk:12.8.0:*:*:*:*:*:
cpe:2.3:a:digium:asterisk:12.8.0:rc1:*:*:*:*:*:
cpe:2.3:a:digium:asterisk:12.8.0:rc2:*:*:*:*:*:
cpe:2.3:a:digium:asterisk:12.8.1:*:*:*:*:*:
cpe:2.3:a:digium:asterisk:13.0.0:*:*:*:*:*:
cpe:2.3:a:digium:asterisk:13.1.0:*:*:*:*:*:
cpe:2.3:a:digium:asterisk:13.1.0:rc1:*:*:*:*:*:
cpe:2.3:a:digium:asterisk:13.1.0:rc2:*:*:*:*:*:
cpe:2.3:a:digium:asterisk:13.2.0:*:*:*:*:*:
cpe:2.3:a:digium:asterisk:13.2.0:rc1:*:*:*:*:*:

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