



CVE-2007-2294

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2007-2294
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-04-26 20:19:00 UTC
Updated	2018-10-16 16:43:00 UTC
Description	The Manager Interface in Asterisk before 1.2.18 and 1.4.x before 1.4.3 allows remote attackers to cause a denial of service

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Asterisk	Asterisk	1.2.0_beta1	All	All	All
Application	Asterisk	Asterisk	1.2.0_beta2	All	All	All
Application	Asterisk	Asterisk	1.2.10	All	All	All
Application	Asterisk	Asterisk	1.2.11	All	All	All
Application	Asterisk	Asterisk	1.2.12	All	All	All
Application	Asterisk	Asterisk	1.2.13	All	All	All
Application	Asterisk	Asterisk	1.2.14	All	All	All
Application	Asterisk	Asterisk	1.2.15	All	All	All
Application	Asterisk	Asterisk	1.2.16	All	All	All
Application	Asterisk	Asterisk	1.2.17	All	All	All
Application	Asterisk	Asterisk	1.2.5	All	All	All
Application	Asterisk	Asterisk	1.2.6	All	All	All
Application	Asterisk	Asterisk	1.2.7	All	All	All
Application	Asterisk	Asterisk	1.2.8	All	All	All
Application	Asterisk	Asterisk	1.2.9	All	All	All
Application	Asterisk	Asterisk	1.4.1	All	All	All
Application	Asterisk	Asterisk	1.4.2	All	All	All

Application	Asterisk	Asterisk	1.4_beta	All	All	All
Application	Asterisk	Asterisk	1.2.0_beta1	All	All	All
Application	Asterisk	Asterisk	1.2.0_beta2	All	All	All
Application	Asterisk	Asterisk	1.2.10	All	All	All
Application	Asterisk	Asterisk	1.2.11	All	All	All
Application	Asterisk	Asterisk	1.2.12	All	All	All
Application	Asterisk	Asterisk	1.2.13	All	All	All
Application	Asterisk	Asterisk	1.2.14	All	All	All
Application	Asterisk	Asterisk	1.2.15	All	All	All
Application	Asterisk	Asterisk	1.2.16	All	All	All
Application	Asterisk	Asterisk	1.2.17	All	All	All
Application	Asterisk	Asterisk	1.2.5	All	All	All
Application	Asterisk	Asterisk	1.2.6	All	All	All
Application	Asterisk	Asterisk	1.2.7	All	All	All
Application	Asterisk	Asterisk	1.2.8	All	All	All
Application	Asterisk	Asterisk	1.2.9	All	All	All
Application	Asterisk	Asterisk	1.4.1	All	All	All
Application	Asterisk	Asterisk	1.4.2	All	All	All
Application	Asterisk	Asterisk	1.4_beta	All	All	All

References						
Reference					Source	Link
Asterisk T.38 SDP Buffer Overflows and Management Interface Denial of Service - Advisories - Secunia					SECUNIA	secunia.com
35369					OSVDB	osvdb.org
Page not found * Open Source Communications Software Asterisk Official Site					CONFIRM	asterisk.org
SecurityFocus					BUGTRAQ	securityfocus.com
Debian -- Security Information -- DSA-1358-1 asterisk					DEBIAN	debian.org
SUSE update for asterisk - Advisories - Secunia					SECUNIA	secunia.com
IBM X-Force Exchange					XF	xforce.ibmcloud.com
Webmail OVH- OVH					VUPEN	ovh.com
CXSecurity - IDS					SREASON	cxsecurity.com
Security Announcement					SUSE	suse.com
SecurityTracker.com Archives - Asterisk Manager Interface NULL Pointer Dereference Lets Remote Users Deny Service					SECTrack	sectrack.com
Asterisk ManagerInterface Manager.Conf Remote Denial of Service Vulnerability					BID	bid.sans.org
CVE Program record					CVE.ORG	cve.org

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

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