



CVE-2006-4345

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

Summary

CVE	CVE-2006-4345
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-08-24 20:04:00 UTC
Updated	2018-10-17 21:36:00 UTC
Description	Stack-based buffer overflow in channels/chan_mgcp.c in MGCP in Asterisk 1.0 through 1.2.10 allows remote attackers to e

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Digium	Asterisk	1.0.0	All	All	All
Application	Digium	Asterisk	1.0.1	All	All	All
Application	Digium	Asterisk	1.0.10	All	All	All
Application	Digium	Asterisk	1.0.2	All	All	All
Application	Digium	Asterisk	1.0.3	All	All	All
Application	Digium	Asterisk	1.0.4	All	All	All
Application	Digium	Asterisk	1.0.5	All	All	All
Application	Digium	Asterisk	1.0.6	All	All	All
Application	Digium	Asterisk	1.0.7	All	All	All
Application	Digium	Asterisk	1.0.8	All	All	All
Application	Digium	Asterisk	1.0.9	All	All	All
Application	Digium	Asterisk	1.0_rc1	All	All	All
Application	Digium	Asterisk	1.0_rc2	All	All	All
Application	Digium	Asterisk	1.2.0_beta1	All	All	All
Application	Digium	Asterisk	1.2.0_beta2	All	All	All
Application	Digium	Asterisk	1.2.10	All	All	All
Application	Digium	Asterisk	1.2.6	All	All	All

Application	Digium	Asterisk	1.2.7	All	All	All
Application	Digium	Asterisk	1.2.8	All	All	All
Application	Digium	Asterisk	1.2.9	All	All	All
Application	Digium	Asterisk	1.0.0	All	All	All
Application	Digium	Asterisk	1.0.1	All	All	All
Application	Digium	Asterisk	1.0.10	All	All	All
Application	Digium	Asterisk	1.0.2	All	All	All
Application	Digium	Asterisk	1.0.3	All	All	All
Application	Digium	Asterisk	1.0.4	All	All	All
Application	Digium	Asterisk	1.0.5	All	All	All
Application	Digium	Asterisk	1.0.6	All	All	All
Application	Digium	Asterisk	1.0.7	All	All	All
Application	Digium	Asterisk	1.0.8	All	All	All
Application	Digium	Asterisk	1.0.9	All	All	All
Application	Digium	Asterisk	1.0_rc1	All	All	All
Application	Digium	Asterisk	1.0_rc2	All	All	All
Application	Digium	Asterisk	1.2.0_beta1	All	All	All
Application	Digium	Asterisk	1.2.0_beta2	All	All	All
Application	Digium	Asterisk	1.2.10	All	All	All
Application	Digium	Asterisk	1.2.6	All	All	All
Application	Digium	Asterisk	1.2.7	All	All	All
Application	Digium	Asterisk	1.2.8	All	All	All
Application	Digium	Asterisk	1.2.9	All	All	All

References						
Reference						Source
ftp.digium.com/pub/asterisk/ChangeLog-1.2.11						CONFIRM
Multiple Vulnerabilities in Asterisk 1.2.10 (Fixed in 1.2.11)						CONFIRM
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH						VUPEN
Gentoo Linux Documentation -- Asterisk: Multiple vulnerabilities						GENTOO
Asterisk MGCP AUEP Response Handling Buffer Overflow - Advisories - Secunia						SECUNIA
labs.musecurity.com/advisories/MU-200608-01.txt						MISC
Gentoo update for asterisk - Advisories - Secunia						SECUNIA
IBM X-Force Exchange						XF
Asterisk Multiple Remote Vulnerabilities						BID

SecurityFocus	BUGTRAQ
SecurityTracker.com Archives - Asterisk Stack Overflow in MGCP Implementation Lets Remote Users Execute Arbitrary Code	SECTrack
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#)