



CVE-2007-6430

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary

CVE	CVE-2007-6430
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-12-20 02:46:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Asterisk Open Source 1.2.x before 1.2.26 and 1.4.x before 1.4.16, and Business Edition B.x.x before B.2.3.6 and C.x.x before C.2.3.6

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

AV:N/AC:M/Au:N/C:P/I:N/A:N

Problem Types: CWE-287 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

AV:N/AC:M/Au:N/C:P/I:N/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Asterisk	Asterisk Business Edition	b.1.3.2	All	All	All

Application	Asterisk	Asterisk Business Edition	b.1.3.3	All	All	All
Application	Asterisk	Asterisk Business Edition	b.2.2.0	All	All	All
Application	Asterisk	Asterisk Business Edition	b.2.2.1	All	All	All
Application	Asterisk	Asterisk Business Edition	b.2.3.1	All	All	All
Application	Asterisk	Asterisk Business Edition	b.2.3.2	All	All	All
Application	Asterisk	Asterisk Business Edition	b.2.3.3	All	All	All
Application	Asterisk	Asterisk Business Edition	b.2.3.4	All	All	All
Application	Asterisk	Asterisk Business Edition	c.1.0beta7	All	All	All
Application	Asterisk	Open Source	1.2.0beta1	All	All	All
Application	Asterisk	Open Source	1.2.0beta2	All	All	All
Application	Asterisk	Open Source	1.2.10	All	All	All
Application	Asterisk	Open Source	1.2.11	All	All	All
Application	Asterisk	Open Source	1.2.13	All	All	All
Application	Asterisk	Open Source	1.2.14	All	All	All
Application	Asterisk	Open Source	1.2.15	All	All	All
Application	Asterisk	Open Source	1.2.16	All	All	All
Application	Asterisk	Open Source	1.2.17	All	All	All
Application	Asterisk	Open Source	1.2.18	All	All	All
Application	Asterisk	Open Source	1.2.19	All	All	All
Application	Asterisk	Open Source	1.2.21	All	All	All
Application	Asterisk	Open Source	1.2.22	All	All	All
Application	Asterisk	Open Source	1.2.23	All	All	All
Application	Asterisk	Open Source	1.2.24	All	All	All
Application	Asterisk	Open Source	1.2.25	All	All	All
Application	Asterisk	Open Source	1.2.5	All	All	All
Application	Asterisk	Open Source	1.2.6	All	All	All
Application	Asterisk	Open Source	1.2.7	All	All	All
Application	Asterisk	Open Source	1.2.8	All	All	All
Application	Asterisk	Open Source	1.2.9	All	All	All
Application	Asterisk	Open Source	1.4.1	All	All	All
Application	Asterisk	Open Source	1.4.10	All	All	All
Application	Asterisk	Open Source	1.4.11	All	All	All
Application	Asterisk	Open Source	1.4.12	All	All	All
Application	Asterisk	Open Source	1.4.13	All	All	All
Application	Asterisk	Open Source	1.4.14	All	All	All
Application	Asterisk	Open Source	1.4.15	All	All	All

Application	Asterisk	Open Source	1.4.2	All	All	All
Application	Asterisk	Open Source	1.4.3	All	All	All
Application	Asterisk	Open Source	1.4.4	All	All	All
Application	Asterisk	Open Source	1.4.5	All	All	All
Application	Asterisk	Open Source	1.4.6	All	All	All
Application	Asterisk	Open Source	1.4.7	All	All	All
Application	Asterisk	Open Source	1.4.8	All	All	All
Application	Asterisk	Open Source	1.4.9	All	All	All
Application	Asterisk	Open Source	1.4beta	All	All	All

Vendor Declared Affected Products					
Source	Vendor	Product	Version	Platforms	
CNA	Na	N/a	affected n/a	Not specified	

References	
Reference	Source
Asterisk Registration Database Security Bypass - Advisories - Secunia	af854a3a-2127-422b-91
SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Information - Secunia.com	af854a3a-2127-422b-91
SecurityTracker.com Archives - Asterisk Lets Remote Users Bypass Host-based Access Controls in Certain Cases	af854a3a-2127-422b-91
[security-announce] SUSE Security Summary Report SUSE-SR:2008:005	af854a3a-2127-422b-91
Asterisk Host-Based Authentication Security Bypass Vulnerability	af854a3a-2127-422b-91
IBM X-Force Exchange	af854a3a-2127-422b-91
www.osvdb.org/39519	af854a3a-2127-422b-91
Debian update for asterisk - Advisories - Secunia	af854a3a-2127-422b-91
Gentoo update for asterisk - Advisories - Secunia	af854a3a-2127-422b-91
SecurityReason - Database matching order permits host-based authentication to be ignored	af854a3a-2127-422b-91
SecurityFocus	af854a3a-2127-422b-91
Debian -- Security Information -- DSA-1525-1 asterisk	af854a3a-2127-422b-91
AST-2007-027	af854a3a-2127-422b-91
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91
Asterisk: Multiple vulnerabilities — Gentoo Linux Documentation	af854a3a-2127-422b-91
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](#)