CVE-2009-0871

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

Summary

CVE	CVE-2009-0871
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-03-11 14:19:00 UTC
Updated	2018-10-10 19:32:00 UTC
Description	The SIP channel driver in Asterisk Open Source 1.4.22, 1.4.23, and 1.4.23.1; 1.6.0 before 1.6.0.6; 1.6.1 before 1.6.1.0-rc2;

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Digium	Asterisk	1.4.22	All	All	All
Application	Digium	Asterisk	1.4.23	All	All	All
Application	Digium	Asterisk	1.4.23.1	All	All	All
Application	Digium	Asterisk	1.6.0	All	All	All
Application	Digium	Asterisk	1.6.0	beta1	All	All
Application	Digium	Asterisk	1.6.0	beta2	All	All
Application	Digium	Asterisk	1.6.0	beta3	All	All
Application	Digium	Asterisk	1.6.0	beta4	All	All
Application	Digium	Asterisk	1.6.0	beta5	All	All
Application	Digium	Asterisk	1.6.0	beta6	All	All
Application	Digium	Asterisk	1.6.0	beta7	All	All
Application	Digium	Asterisk	1.6.0	beta7.1	All	All
Application	Digium	Asterisk	1.6.0	beta8	All	All
Application	Digium	Asterisk	1.6.0	beta9	All	All
Application	Digium	Asterisk	1.6.0	rc4	All	All
Application	Digium	Asterisk	1.6.0	rc5	All	All
Application	Digium	Asterisk	1.6.0	rc6	All	All

Application	Digium	Asterisk	1.6.0.1	All	All	All
Application	Digium	Asterisk	1.6.0.2	All	All	All
Application	Digium	Asterisk	1.6.0.3	All	All	All
Application	Digium	Asterisk	1.6.0.3	rc1	All	All
Application	Digium	Asterisk	1.6.0.4	rc1	All	All
Application	Digium	Asterisk	1.6.0.5	All	All	All
Application	Digium	Asterisk	1.6.1	All	All	All
Application	Digium	Asterisk	1.6.1	beta1	All	All
Application	Digium	Asterisk	1.6.1	beta2	All	All
Application	Digium	Asterisk	1.6.1	beta3	All	All
Application	Digium	Asterisk	1.6.1	beta4	All	All
Application	Digium	Asterisk	1.6.1	rc1	All	All
Application	Digium	Asterisk	c.2.3	-	business	All
Application	Digium	Asterisk	1.4.22	All	All	All
Application	Digium	Asterisk	1.4.23	All	All	All
Application	Digium	Asterisk	1.4.23.1	All	All	All
Application	Digium	Asterisk	1.6.0	All	All	All
Application	Digium	Asterisk	1.6.0	beta1	All	All
Application	Digium	Asterisk	1.6.0	beta2	All	All
Application	Digium	Asterisk	1.6.0	beta3	All	All
Application	Digium	Asterisk	1.6.0	beta4	All	All
Application	Digium	Asterisk	1.6.0	beta5	All	All
Application	Digium	Asterisk	1.6.0	beta6	All	All
Application	Digium	Asterisk	1.6.0	beta7	All	All
Application	Digium	Asterisk	1.6.0	beta7.1	All	All
Application	Digium	Asterisk	1.6.0	beta8	All	All
Application	Digium	Asterisk	1.6.0	beta9	All	All
Application	Digium	Asterisk	1.6.0	rc4	All	All
Application	Digium	Asterisk	1.6.0	rc5	All	All
Application	Digium	Asterisk	1.6.0	rc6	All	All
Application	Digium	Asterisk	1.6.0.1	All	All	All
Application	Digium	Asterisk	1.6.0.2	All	All	All
Application	Digium	Asterisk	1.6.0.3	All	All	All
Application	Digium	Asterisk	1.6.0.3	rc1	All	All
Application	Digium	Asterisk	1.6.0.4	rc1	All	All

Application	Digium	Asterisk	1.6.0.5	All	All	All
Application	Digium	Asterisk	1.6.1	All	All	All
Application	Digium	Asterisk	1.6.1	beta1	All	All
Application	Digium	Asterisk	1.6.1	beta2	All	All
Application	Digium	Asterisk	1.6.1	beta3	All	All
Application	Digium	Asterisk	1.6.1	beta4	All	All
Application	Digium	Asterisk	1.6.1	rc1	All	All
Application	Digium	Asterisk	c.2.3	-	business	All

References

Reference
AST-2009-002
[ASTERISK-13525] Asterisk crash with looped request and pedantic=yes - Digium/Asterisk JIRA
Asterisk "pedantic" SIP Processing Denial of Service - Secunia Advisories - Vulnerability Information - Secunia.com
Asterisk Bug in Processing SIP INVITE Request with NULL Header Values Lets Remote Authenticated Users Deny Service - SecurityTracker
52568
SecurityFocus
Asterisk Pedantic Mode SIP Channel Driver INVITE Header Remote Denial of Service Vulnerability
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
[ASTERISK-12768] [patch] Asterisk crash getting fax by sip channel - Digium/Asterisk JIRA
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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