



CVE-2017-16671

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

| | |
|------------------------|--|
| CVE | CVE-2017-16671 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2017-11-09 00:29:00 UTC |
| Updated | 2018-11-25 11:29:00 UTC |
| Description | A Buffer Overflow issue was discovered in Asterisk Open Source 13 before 13.18.1, 14 before 14.7.1, and 15 before 15.1.1 |

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|--------|--------------------|---------|-----------|---------|----------|
| Application | Digium | Asterisk | All | All | All | All |
| Application | Digium | Asterisk | All | All | All | All |
| Application | Digium | Certified Asterisk | 13.13.0 | All | All | All |
| Application | Digium | Certified Asterisk | 13.13.0 | cert1 | All | All |
| Application | Digium | Certified Asterisk | 13.13.0 | cert1_rc1 | All | All |
| Application | Digium | Certified Asterisk | 13.13.0 | cert1_rc2 | All | All |
| Application | Digium | Certified Asterisk | 13.13.0 | cert1_rc3 | All | All |
| Application | Digium | Certified Asterisk | 13.13.0 | cert1_rc4 | All | All |
| Application | Digium | Certified Asterisk | 13.13.0 | cert2 | All | All |
| Application | Digium | Certified Asterisk | 13.13.0 | cert3 | All | All |
| Application | Digium | Certified Asterisk | 13.13.0 | cert4 | All | All |
| Application | Digium | Certified Asterisk | 13.13.0 | cert5 | All | All |
| Application | Digium | Certified Asterisk | 13.13.0 | cert6 | All | All |
| Application | Digium | Certified Asterisk | 13.13.0 | All | All | All |
| Application | Digium | Certified Asterisk | 13.13.0 | cert1 | All | All |
| Application | Digium | Certified Asterisk | 13.13.0 | cert1_rc1 | All | All |
| Application | Digium | Certified Asterisk | 13.13.0 | cert1_rc2 | All | All |

| | | | | | | |
|-------------|------------------------|------------------------------------|---------|-----------|-----|-----|
| Application | Digium | Certified Asterisk | 13.13.0 | cert1_rc3 | All | All |
| Application | Digium | Certified Asterisk | 13.13.0 | cert1_rc4 | All | All |
| Application | Digium | Certified Asterisk | 13.13.0 | cert2 | All | All |
| Application | Digium | Certified Asterisk | 13.13.0 | cert3 | All | All |
| Application | Digium | Certified Asterisk | 13.13.0 | cert4 | All | All |
| Application | Digium | Certified Asterisk | 13.13.0 | cert5 | All | All |
| Application | Digium | Certified Asterisk | 13.13.0 | cert6 | All | All |

References

| Reference | Source | Link |
|--|---------|--|
| Debian -- Security Information -- DSA-4076-1 asterisk | DEBIAN | www.debian.org |
| Multiple Asterisk Products CDR Remote Buffer Overflow Vulnerability | BID | www.securityfocus.com/bid |
| AST-2017-010 | CONFIRM | downloads.digium.com |
| [ASTERISK-27337] chan_sip: Security vulnerability with client code header (revisited) - Digium/Asterisk JIRA | CONFIRM | issues.asterisk.org |
| Asterisk: Multiple vulnerabilities (GLSA 201811-11) — Gentoo security | GENTOO | security.gentoo.org |
| CVE Program record | CVE.ORG | www.cve.org |
| NVD vulnerability detail | NVD | nvd.nist.gov |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

710292 Gentoo Linux Asterisk Multiple Vulnerabilities (GLSA 201811-11)

© 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](#).

CVE.report and Source URL Uptime Status status.cve.report