



# CVE-2021-26713

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

## Summary

<b>CVE</b>	CVE-2021-26713
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-02-19 20:15:00 UTC
<b>Updated</b>	2021-02-26 17:02:00 UTC
<b>Description</b>	A stack-based buffer overflow in res_rtp_asterisk.c in Sangoma Asterisk before 16.16.1, 17.x before 17.9.2, and 18.x before

## Risk And Classification

**Problem Types:** CWE-787

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Digium</a>	<a href="#">Asterisk</a>	All	All	All	All
Application	<a href="#">Digium</a>	<a href="#">Asterisk</a>	All	All	All	All
Application	<a href="#">Digium</a>	<a href="#">Certified Asterisk</a>	16.8	-	All	All
Application	<a href="#">Digium</a>	<a href="#">Certified Asterisk</a>	16.8	cert1-rc1	All	All
Application	<a href="#">Digium</a>	<a href="#">Certified Asterisk</a>	16.8	cert1-rc2	All	All
Application	<a href="#">Digium</a>	<a href="#">Certified Asterisk</a>	16.8	cert1-rc3	All	All
Application	<a href="#">Digium</a>	<a href="#">Certified Asterisk</a>	16.8	cert1-rc4	All	All
Application	<a href="#">Digium</a>	<a href="#">Certified Asterisk</a>	16.8	cert2	All	All
Application	<a href="#">Digium</a>	<a href="#">Certified Asterisk</a>	16.8	cert3	All	All
Application	<a href="#">Digium</a>	<a href="#">Certified Asterisk</a>	16.8	cert4	All	All
Application	<a href="#">Digium</a>	<a href="#">Certified Asterisk</a>	16.8	cert4-rc1	All	All
Application	<a href="#">Digium</a>	<a href="#">Certified Asterisk</a>	16.8	cert4-rc2	All	All
Application	<a href="#">Digium</a>	<a href="#">Certified Asterisk</a>	16.8	cert4-rc3	All	All
Application	<a href="#">Digium</a>	<a href="#">Certified Asterisk</a>	16.8	cert4-rc4	All	All
Application	<a href="#">Digium</a>	<a href="#">Certified Asterisk</a>	16.8	cert5	All	All
Application	<a href="#">Digium</a>	<a href="#">Certified Asterisk</a>	16.8	-	All	All
Application	<a href="#">Digium</a>	<a href="#">Certified Asterisk</a>	16.8	cert1-rc1	All	All

Application	Digium	Certified Asterisk	16.8	cert1-rc2	All	All
Application	Digium	Certified Asterisk	16.8	cert1-rc3	All	All
Application	Digium	Certified Asterisk	16.8	cert1-rc4	All	All
Application	Digium	Certified Asterisk	16.8	cert2	All	All
Application	Digium	Certified Asterisk	16.8	cert3	All	All
Application	Digium	Certified Asterisk	16.8	cert4	All	All
Application	Digium	Certified Asterisk	16.8	cert4-rc1	All	All
Application	Digium	Certified Asterisk	16.8	cert4-rc2	All	All
Application	Digium	Certified Asterisk	16.8	cert4-rc3	All	All
Application	Digium	Certified Asterisk	16.8	cert4-rc4	All	All
Application	Digium	Certified Asterisk	16.8	cert5	All	All

## References

Reference	Source	Link
AST-2021-004	MISC	<a href="#">dow</a>
Index of /pub/security	MISC	<a href="#">dow</a>
[ASTERISK-29205] res_rtp_asterisk: Asterisk crashes when making hold/unhold from webrtc client - Digium/Asterisk JIRA	MISC	<a href="#">issu</a>
CVE Program record	CVE.ORG	<a href="#">ww</a>
NVD vulnerability detail	NVD	<a href="#">nvd</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[500035](#) Alpine Linux Security Update for asterisk

[501378](#) Alpine Linux Security Update for asterisk

[503868](#) Alpine Linux Security Update for asterisk

© 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](#)