CVE-2018-17281

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2018-17281
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-09-24 22:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	There is a stack consumption vulnerability in the res_http_websocket.so module of Asterisk through 13.23.0, 14.7.x through

Risk And Classification

Problem Types: CWE-400

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Digium	Asterisk	All	All	All	All
Application	Digium	Asterisk	All	All	All	All
Application	Digium	Asterisk	All	All	All	All
Application	Digium	Certified Asterisk	11.6	cert12	All	All
Application	Digium	Certified Asterisk	11.6	cert13	All	All
Application	Digium	Certified Asterisk	11.6	cert14	All	All
Application	Digium	Certified Asterisk	11.6	cert15	All	All
Application	Digium	Certified Asterisk	11.6	cert16	All	All
Application	Digium	Certified Asterisk	11.6	cert17	All	All
Application	Digium	Certified Asterisk	11.6	cert18	All	All
Application	Digium	Certified Asterisk	13.1	cert3	All	All
Application	Digium	Certified Asterisk	13.1	cert4	All	All
Application	Digium	Certified Asterisk	13.1	cert5	All	All

Application	Digium	Certified Asterisk	13.1	cert6	All	All
Application	Digium	Certified Asterisk	13.1	cert7	All	All
Application	Digium	Certified Asterisk	13.1	cert8	All	All
Application	Digium	Certified Asterisk	13.13	cert1	All	All
Application	Digium	Certified Asterisk	13.13	cert2	All	All
Application	Digium	Certified Asterisk	13.13	cert3	All	All
Application	Digium	Certified Asterisk	13.13	cert4	All	All
Application	Digium	Certified Asterisk	13.13	cert5	All	All
Application	Digium	Certified Asterisk	13.13	cert6	All	All
Application	Digium	Certified Asterisk	13.13	cert7	All	All
Application	Digium	Certified Asterisk	13.13	cert8	All	All
Application	Digium	Certified Asterisk	13.13	cert9	All	All
Application	Digium	Certified Asterisk	13.21	cert1	All	All
Application	Digium	Certified Asterisk	13.21	cert2	All	All
Application	Digium	Certified Asterisk	13.8	cert1	All	All
Application	Digium	Certified Asterisk	13.8	cert2	All	All
Application	Digium	Certified Asterisk	13.8	cert3	All	All
Application	Digium	Certified Asterisk	13.8	cert4	All	All
Application	Digium	Certified Asterisk	11.6	cert12	All	All
Application	Digium	Certified Asterisk	11.6	cert13	All	All
Application	Digium	Certified Asterisk	11.6	cert14	All	All
Application	Digium	Certified Asterisk	11.6	cert15	All	All
Application	Digium	Certified Asterisk	11.6	cert16	All	All
Application	Digium	Certified Asterisk	11.6	cert17	All	All
Application	Digium	Certified Asterisk	11.6	cert18	All	All
Application	Digium	Certified Asterisk	13.1	cert3	All	All
Application	Digium	Certified Asterisk	13.1	cert4	All	All
Application	Digium	Certified Asterisk	13.1	cert5	All	All
Application	Digium	Certified Asterisk	13.1	cert6	All	All
Application	Digium	Certified Asterisk	13.1	cert7	All	All
Application	Digium	Certified Asterisk	13.1	cert8	All	All
Application	Digium	Certified Asterisk	13.13	cert1	All	All
Application	Digium	Certified Asterisk	13.13	cert2	All	All
Application	Digium	Certified Asterisk	13.13	cert3	All	All
Application	Digium	Certified Asterisk	13.13	cert4	All	All

Application	Digium	Certified Asterisk	13.13	cert5	All	All
Application	Digium	Certified Asterisk	13.13	cert6	All	All
Application	Digium	Certified Asterisk	13.13	cert7	All	All
Application	Digium	Certified Asterisk	13.13	cert8	All	All
Application	Digium	Certified Asterisk	13.13	cert9	All	All
Application	Digium	Certified Asterisk	13.21	cert1	All	All
Application	Digium	Certified Asterisk	13.21	cert2	All	All
Application	Digium	Certified Asterisk	13.8	cert1	All	All
Application	Digium	Certified Asterisk	13.8	cert2	All	All
Application	Digium	Certified Asterisk	13.8	cert3	All	All
Application	Digium	Certified Asterisk	13.8	cert4	All	All

References

Reference	Source
Asterisk Stack Overflow in HTTP Websocket Upgrade Lets Remote Users Cause the Target Service to Crash - SecurityTracker	SECTRACK
Multiple Asterisk Products CVE-2018-17281 Remote Stack Overflow Vulnerability	BID
Debian -- Security Information -- DSA-4320-1 asterisk	DEBIAN
Full Disclosure: AST-2018-009: Remote crash vulnerability in HTTP websocket upgrade	FULLDISC
Asterisk Project Security Advisory - AST-2018-009 ≈ Packet Storm	MISC
[ASTERISK-28013] res_http_websocket: Crash when reading HTTP Upgrade requests - Digium/Asterisk JIRA	CONFIRM
[SECURITY] [DLA 1523-1] asterisk security update	MLIST
AST-2018-009	CONFIRM
Bugtraq: AST-2018-009: Remote crash vulnerability in HTTP websocket upgrade	BUGTRAQ
Asterisk: Multiple vulnerabilities (GLSA 201811-11) — Gentoo security	GENTOO
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

690609 Free Berkeley Software Distribution (FreeBSD) Security Update for asterisk (77f67b46-bd75-11e8-81b6-001999f8d30b)

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

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