



CVE-2020-28361

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

Summary

CVE	CVE-2020-28361
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-11-18 14:15:00 UTC
Updated	2020-12-03 13:07:00 UTC
Description	Kamailio before 5.4.0, as used in Sip Express Router (SER) in Sippy Softswitch 4.5 through 5.2 and other products, allows

Risk And Classification

Problem Types: CWE-444

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kamailio	Kamailio	All	All	All	All
Application	Kamailio	Kamailio	All	All	All	All

References

Reference	Source	Link	Tags
Kamailio 5.4.0 Header Smuggling ≈ Packet Storm	MISC	packetstormsecurity.com	Exploit, Third Party Advisory, VDB Entry
Sign into : Sippy Software, Inc.	MISC	support.sippysoft.com	Permissions Required
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[180629](#) Debian Security Update for kamailio (CVE-2020-28361)

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