



CVE-2020-27507

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2020-27507
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-15 20:15:00 UTC
Updated	2023-05-30 19:15:00 UTC
Description	The Kamailio SIP before 5.5.0 server mishandles INVITE requests with duplicated fields and overlength tag, leading to a bu

Risk And Classification

Problem Types: CWE-120

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
Crash on qm_debug_check_frag() on INVITE · Issue #2503 · kamailio/kamailio · GitHub	MISC	github.com	
tm: do not add duplicate headers in local requests · kamailio/kamailio@ada3701 · GitHub	MISC	github.com	
[SECURITY] [DLA 3438-1] kamailio security update	MLIST	lists.debian.org	
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

[181813](#) Debian Security Update for kamailio (DLA 3438-1)

[199477](#) Ubuntu Security Notification for Kamailio Vulnerabilities (USN-6022-1)

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)