



CVE-2023-27598

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

Summary

CVE	CVE-2023-27598
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-15 21:15:00 UTC
Updated	2023-03-21 19:14:00 UTC
Description	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. Prior to versions 3.1.7 and 3.2.4, sending a malformed SIP message to the server could cause a denial of service. This vulnerability is caused by a buffer overflow in the parse_via() function. The vulnerability is present in versions 3.1.7 and 3.2.4, and is fixed in version 3.1.8 and 3.2.5.

Risk And Classification

Problem Types: CWE-908

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
Vulnerability in the parse_via() function · Advisory · OpenSIPS/opensips · GitHub	MISC	github.com	
[core] fix parse_via() parsing · OpenSIPS/opensips@ab611f7 · GitHub	MISC	github.com	
opensips.org/pub/audit-2022/opensips-audit-technical-report-full.pdf	MISC	opensips.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.

There are currently no legacy QID mappings associated with this CVE.

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