



CVE-2017-7853

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

Summary

CVE	CVE-2017-7853
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-04-13 16:59:00 UTC
Updated	2017-11-04 01:29:00 UTC
Description	In libosip2 in GNU oSIP 4.1.0 and 5.0.0, a malformed SIP message can lead to a heap buffer overflow in the msg_osip_boc

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Osip	5.0.0	All	All	All
Application	Gnu	Osip	5.0.0	All	All	All

References

Reference	Source	Link	Tags
The oSIP library - Support: sr #109265, SIP message body length underflow... [Savannah]	CONFIRM	savannah.gnu.org	Issue Tra
GNU oSIP 'osipparser2/osip_message_parse.c' Heap Buffer Overflow Vulnerability	BID	www.securityfocus.com	Third Par
Debian -- Security Information -- DSA-3879-1 libosip2	DEBIAN	www.debian.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

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

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