



CVE-2023-25950

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

Summary

CVE	CVE-2023-25950
State	PUBLIC
Assigner	vultures@jpcert.or.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-04-11 09:15:00 UTC
Updated	2023-11-07 04:09:00 UTC
Description	HTTP request/response smuggling vulnerability in HAProxy version 2.7.0, and 2.6.1 to 2.6.7 allows a remote attacker to alt

Risk And Classification

Problem Types: CWE-444

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Haproxy	Haproxy	2.7.0	All	All	All
Application	Haproxy	Haproxy	All	All	All	All

References

Reference	Source	Link	Tags
Repositories - haproxy-2.7.git/commit	MISC	git.haproxy.org	Mailing List, Patch
JVN#38170084: HAProxy vulnerable to HTTP request/response smuggling	MISC	jvn.jp	Third Party Advisory, VDB Entr
Repositories		git.haproxy.org	
www.haproxy.org	MISC	www.haproxy.org	Product
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

[182482](#) Debian Security Update for haproxy (CVE-2023-25950)

© [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](#)