



CVE-2021-39240

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2021-39240
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-17 19:15:00 UTC
Updated	2023-11-07 03:37:00 UTC
Description	An issue was discovered in HAProxy 2.2 before 2.2.16, 2.3 before 2.3.13, and 2.4 before 2.4.3. It does not ensure that the s

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	11.0	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Application	Haproxy	Haproxy	All	All	All	All

References

Reference	Source	Link	Ta
Repositories - haproxy.git/commit	MISC	git.haproxy.org	
[SECURITY] Fedora 34 Update: haproxy-2.3.13-1.fc34 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[SECURITY] Fedora 33 Update: haproxy-2.2.16-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
[ANNOUNCE] HTTP/2 vulnerabilities from 2.0 to 2.5-dev		www.mail-archive.com	
[SECURITY] Fedora 34 Update: haproxy-2.3.13-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
Repositories - haproxy.git/commit		git.haproxy.org	
Debian -- Security Information -- DSA-4960-1 haproxy	DEBIAN	www.debian.org	
Repositories - haproxy.git/commit	MISC	git.haproxy.org	
[SECURITY] Fedora 33 Update: haproxy-2.2.16-1.fc33 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[ANNOUNCE] HTTP/2 vulnerabilities from 2.0 to 2.5-dev	MISC	www.mail-archive.com	

Repositories - haproxy.git/commit		git.haproxy.org	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [184421](#) Debian Security Update for haproxy (CVE-2021-39240)
- [239873](#) Red Hat OpenShift Container Platform 4.9 Security Update (RHSA-2021:4118)
- [239987](#) Red Hat OpenShift Container Platform 4.8 Security Update (RHSA-2021:5208)
- [281856](#) Fedora Security Update for haproxy (FEDORA-2021-3ab4512c98)
- [281857](#) Fedora Security Update for haproxy (FEDORA-2021-e6557245e8)
- [356275](#) Amazon Linux Security Advisory for haproxy2 : ALASHAPROXY2-2023-005
- [356499](#) Amazon Linux Security Advisory for haproxy2 : ALAS2HAPROXY2-2023-005
- [770124](#) Red Hat OpenShift Container Platform 4.9 Security Update (RHSA-2021:4118)
- [770130](#) Red Hat OpenShift Container Platform 4.8 Security Update (RHSA-2021:5208)

© [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](#).

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