CVE-2022-0711

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-0711
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-02 22:15:00 UTC
Updated	2023-11-07 03:41:00 UTC
Description	A flaw was found in the way HAProxy processed HTTP responses containing the "Set-Cookie2" header. This flaw could allo

Risk And Classification

Problem Types: CWE-835

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	11.0	All	All	All
Application	Haproxy	Haproxy	All	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Application	Redhat	Openshift Container Platform	4.0	All	All	All
Application	Redhat	Software Collections	-	All	All	All

References

Reference	Source	Link
Debian -- Security Information -- DSA-5102-1 haproxy	DEBIAN	www.debi
BUG/MAJOR: http/htx: prevent unbounded loop in http_manage_server_sid… · haproxy/haproxy@bfb15ab · GitHub	MISC	github.cor
[ANNOUNCE] haproxy-2.5.2		www.mail
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.re
[ANNOUNCE] haproxy-2.5.2	MISC	www.mail
CVE Program record	CVE.ORG	www.cve.
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

179145 Debian Security Update for haproxy (DSA 5102-1)

183652 Debian Security Update for haproxy (CVE-2022-0711)

198687 Ubuntu Security Notification for HAProxy Vulnerability (USN-5312-1)

240192 Red Hat OpenShift Container Platform 4.9 Security Update (RHSA-2022:1021)

240213 Red Hat OpenShift Container Platform 4.8 Security Update (RHSA-2022:1153)

240227 Red Hat OpenShift Container Platform 4.7 Security Update (RHSA-2022:1336)

240264 Red Hat OpenShift Container Platform 4.6 Security Update (RHSA-2022:1620)

356222 Amazon Linux Security Advisory for haproxy2 : ALASHAPROXY2-2023-001

356489 Amazon Linux Security Advisory for haproxy2 : ALAS2HAPROXY2-2023-001

500241 Alpine Linux Security Update for haproxy

671741 EulerOS Security Update for haproxy (EulerOS-SA-2022-1806)

671753 EulerOS Security Update for haproxy (EulerOS-SA-2022-1789)

671781 EulerOS Security Update for haproxy (EulerOS-SA-2022-1866)

671820 EulerOS Security Update for haproxy (EulerOS-SA-2022-1842)

753326 SUSE Enterprise Linux Security Update for haproxy (SUSE-SU-2022:2277-1)

770146 Red Hat OpenShift Container Platform 4.9 Security Update (RHSA-2022:1021)

770147 Red Hat OpenShift Container Platform 4.8 Security Update (RHSA-2022:1153)

770149 Red Hat OpenShift Container Platform 4.7 Security Update (RHSA-2022:1336)

770151 Red Hat OpenShift Container Platform 4.6 Security Update (RHSA-2022:1620)

901231 Common Base Linux Mariner (CBL-Mariner) Security Update for haproxy (8899)

906348 Common Base Linux Mariner (CBL-Mariner) Security Update for haproxy (8899-2)

© 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 registred 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