



CVE-2019-19330

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2019-19330 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2019-11-27 16:15:00 UTC |
| Updated | 2023-11-07 03:07:00 UTC |
| Description | The HTTP/2 implementation in HAProxy before 2.0.10 mishandles headers, as demonstrated by carriage return (CR, ASCII |

Risk And Classification

Problem Types: CWE-74

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|---------------------------|------------------------------|---------|--------|---------|----------|
| Operating System | Canonical | Ubuntu Linux | 18.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 19.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 19.10 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 18.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 19.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 19.10 | All | All | All |
| Operating System | Debian | Debian Linux | 10.0 | All | All | All |
| Operating System | Debian | Debian Linux | 10.0 | All | All | All |
| Application | Haproxy | Haproxy | All | All | All | All |
| Application | Haproxy | Haproxy | All | All | All | All |

References

| Reference | Source | Link | Tags |
|--|--------|---|---------------------|
| RFC 7540 - Hypertext Transfer Protocol Version 2 (HTTP/2) | MISC | tools.ietf.org | Third Party Advisor |
| Repositories - haproxy-2.0.git/commit | | git.haproxy.org | |
| Debian -- Security Information -- DSA-4577-1 haproxy | DEBIAN | www.debian.org | Third Party Advisor |
| HAProxy: Remote execution of arbitrary code (GLSA 202004-01) — Gentoo security | GENTOO | security.gentoo.org | |

| | | | |
|--|---------|---|-----------------------|
| USN-4212-1: HAProxy vulnerability Ubuntu security notices Ubuntu | UBUNTU | usn.ubuntu.com | Third Party Advisor |
| Bugtraq: [SECURITY] [DSA 4577-1] haproxy security update | BUGTRAQ | seclists.org | Mailing List, Third F |
| Repositories - haproxy.git/commit | | git.haproxy.org | |
| Repositories - haproxy-2.0.git/commit | MISC | git.haproxy.org | Patch |
| Repositories - haproxy.git/commit | | git.haproxy.org | |
| Repositories - haproxy.git/commit | MISC | git.haproxy.org | Patch |
| Repositories - haproxy.git/commit | MISC | git.haproxy.org | Patch |
| 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

[770024](#) Red Hat OpenShift Container Platform 4.4.3 Security Update (RHSA-2020:1936)

© [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