



CVE-2018-20615

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

Summary

CVE	CVE-2018-20615
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-03-21 16:00:00 UTC
Updated	2023-11-07 02:56:00 UTC
Description	An out-of-bounds read issue was discovered in the HTTP/2 protocol decoder in HAProxy 1.8.x and 1.9.x through 1.9.0 which

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	All	All	All
Application	Haproxy	Haproxy	1.9.0	-	All	All
Application	Haproxy	Haproxy	1.9.0	dev0	All	All
Application	Haproxy	Haproxy	1.9.0	dev1	All	All
Application	Haproxy	Haproxy	1.9.0	dev10	All	All
Application	Haproxy	Haproxy	1.9.0	dev11	All	All
Application	Haproxy	Haproxy	1.9.0	dev2	All	All
Application	Haproxy	Haproxy	1.9.0	dev3	All	All
Application	Haproxy	Haproxy	1.9.0	dev4	All	All
Application	Haproxy	Haproxy	1.9.0	dev5	All	All
Application	Haproxy	Haproxy	1.9.0	dev6	All	All
Application	Haproxy	Haproxy	1.9.0	dev7	All	All

Application	Haproxy	Haproxy	1.9.0	dev8	All	All
Application	Haproxy	Haproxy	1.9.0	dev9	All	All
Application	Haproxy	Haproxy	1.9.0	-	All	All
Application	Haproxy	Haproxy	1.9.0	dev0	All	All
Application	Haproxy	Haproxy	1.9.0	dev1	All	All
Application	Haproxy	Haproxy	1.9.0	dev10	All	All
Application	Haproxy	Haproxy	1.9.0	dev11	All	All
Application	Haproxy	Haproxy	1.9.0	dev2	All	All
Application	Haproxy	Haproxy	1.9.0	dev3	All	All
Application	Haproxy	Haproxy	1.9.0	dev4	All	All
Application	Haproxy	Haproxy	1.9.0	dev5	All	All
Application	Haproxy	Haproxy	1.9.0	dev6	All	All
Application	Haproxy	Haproxy	1.9.0	dev7	All	All
Application	Haproxy	Haproxy	1.9.0	dev8	All	All
Application	Haproxy	Haproxy	1.9.0	dev9	All	All
Application	Haproxy	Haproxy	All	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.4	All	All	All
Operating System	Redhat	Enterprise Linux	7.5	All	All	All
Operating System	Redhat	Enterprise Linux	7.6	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.4	All	All	All
Operating System	Redhat	Enterprise Linux	7.5	All	All	All
Operating System	Redhat	Enterprise Linux	7.6	All	All	All
Application	Redhat	Openshift Container Platform	3.11	All	All	All
Application	Redhat	Openshift Container Platform	3.11	All	All	All

References

Reference	Source	Link	Tags
[ANNOUNCE] haproxy-1.8.17		www.mail-archive.com	
[security-announce] openSUSE-SU-2019:0166-1: important: Security update	MLIST	lists.opensuse.org	Mailing List, Third Party
[ANNOUNCE] haproxy-1.8.17	MLIST	www.mail-archive.com	Mailing List, Third Party
Red Hat Customer Portal	REDHAT	access.redhat.com	Third Party Advisory

USN-3858-1: HAProxy vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com	Third Party Advisory
HAProxy CVE-2018-20615 Remote Denial of Service Vulnerability	BID	www.securityfocus.com	Third Party Advisory, V
Red Hat Customer Portal	REDHAT	access.redhat.com	Third Party Advisory
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.

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

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report