CVE-2013-1912

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2013-1912
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-04-10 15:55:00 UTC
Updated	2013-12-01 04:27:00 UTC
Description	Buffer overflow in HAProxy 1.4 through 1.4.22 and 1.5-dev through 1.5-dev17, when HTTP keep-alive is enabled, using HT

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Haproxy	Haproxy	1.4	All	All	All
Application	Haproxy	Haproxy	1.4.20	All	All	All
Application	Haproxy	Haproxy	1.4.22	All	All	All
Application	Haproxy	Haproxy	1.5	dev	All	All
Application	Haproxy	Haproxy	1.5	dev17	All	All
Application	Haproxy	Haproxy	1.4	All	All	All
Application	Haproxy	Haproxy	1.4.20	All	All	All
Application	Haproxy	Haproxy	1.4.22	All	All	All
Application	Haproxy	Haproxy	1.5	dev	All	All
Application	Haproxy	Haproxy	1.5	dev17	All	All

References

Reference	Source	Link
Red Hat Customer Portal	REDHAT	rhn.redhat.com
oss-security - CVE-2013-1912 : haproxy may crash on TCP content inspection rules	MLIST	www.openwall.com
[SECURITY] Fedora 17 Update: haproxy-1.4.23-1.fc17	FEDORA	lists.fedoraproject.(
Red Hat Customer Portal	REDHAT	rhn.redhat.com

Security Advisory SA52725 - HAProxy HTTP Request Processing Denial of Service Vulnerability - Secunia	SECUNIA	secunia.com
Debian -- Security Information -- DSA-2711-1 haproxy	DEBIAN	www.debian.org
HAProxy 'tcp-request content' CVE-2013-1912 Buffer Overflow Vulnerability	BID	www.securityfocus
[SECURITY] Fedora 19 Update: haproxy-1.4.23-2.fc19	FEDORA	lists.fedoraproject.(
[SECURITY] Fedora 18 Update: haproxy-1.4.23-1.fc18	FEDORA	lists.fedoraproject.(
USN-1800-1: HAProxy vulnerabilities | Ubuntu	UBUNTU	www.ubuntu.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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