CVE-2018-0500

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

Summary

CVE	CVE-2018-0500
State	PUBLIC
Assigner	security@debian.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-07-11 13:29:00 UTC
Updated	2020-08-24 17:37:00 UTC
Description	Curl_smtp_escape_eob in lib/smtp.c in curl 7.54.1 to and including curl 7.60.0 has a heap-based buffer overflow that might

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	17.10	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	17.10	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Application	Haxx	Curl	All	All	All	All

References

Reference	Sourc
USN-3710-1: curl vulnerability | Ubuntu security notices	UBUN
smtp: use the upload buffer size for scratch buffer malloc · curl/curl@ba1dbd7 · GitHub	CONF
curl Buffer Overflow in Curl_smtp_escape_eob() Lets Remote Users Execute Arbitrary Code on the Target System - SecurityTracker	SECTI
Red Hat Customer Portal	REDH
cURL:Heap-based Buffer Overflow (GLSA 201807-04) — Gentoo Security	GENT
curl - SMTP send heap buffer overflow - CVE-2018-0500	CONF
CVE Program record	CVE.C
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

500124 Alpine Linux Security Update for curl

503779 Alpine Linux Security Update for curl

710283 Gentoo Linux cURL Heap-based buffer overflow Vulnerability (GLSA 201807-04)

© 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.

Free CVE JSON API cve.report/api

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