



CVE-2014-0138

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

Summary

CVE	CVE-2014-0138
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-04-15 14:55:04 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The default configuration in cURL and libcurl 7.10.6 before 7.36.0 re-uses (1) SCP, (2) SFTP, (3) POP3, (4) POP3S, (5) IM.

Risk And Classification

Primary CVSS: v2.0 6.4 from nvd@nist.gov

AV:N/AC:L/Au:N/C:P/I:P/A:N

Problem Types: CWE-287 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

None

AV:N/AC:L/Au:N/C:P/I:P/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	7.0	All	All	All

Application	Haxx	Curl	7.10.6	All	All	All
Application	Haxx	Curl	7.10.7	All	All	All
Application	Haxx	Curl	7.10.8	All	All	All
Application	Haxx	Curl	7.11.0	All	All	All
Application	Haxx	Curl	7.11.1	All	All	All
Application	Haxx	Curl	7.11.2	All	All	All
Application	Haxx	Curl	7.12.0	All	All	All
Application	Haxx	Curl	7.12.1	All	All	All
Application	Haxx	Curl	7.12.2	All	All	All
Application	Haxx	Curl	7.12.3	All	All	All
Application	Haxx	Curl	7.13.0	All	All	All
Application	Haxx	Curl	7.13.1	All	All	All
Application	Haxx	Curl	7.13.2	All	All	All
Application	Haxx	Curl	7.14.0	All	All	All
Application	Haxx	Curl	7.14.1	All	All	All
Application	Haxx	Curl	7.15.0	All	All	All
Application	Haxx	Curl	7.15.1	All	All	All
Application	Haxx	Curl	7.15.2	All	All	All
Application	Haxx	Curl	7.15.3	All	All	All
Application	Haxx	Curl	7.15.4	All	All	All
Application	Haxx	Curl	7.15.5	All	All	All
Application	Haxx	Curl	7.16.0	All	All	All
Application	Haxx	Curl	7.16.1	All	All	All
Application	Haxx	Curl	7.16.2	All	All	All
Application	Haxx	Curl	7.16.3	All	All	All
Application	Haxx	Curl	7.16.4	All	All	All
Application	Haxx	Curl	7.17.0	All	All	All
Application	Haxx	Curl	7.17.1	All	All	All
Application	Haxx	Curl	7.18.0	All	All	All
Application	Haxx	Curl	7.18.1	All	All	All
Application	Haxx	Curl	7.18.2	All	All	All
Application	Haxx	Curl	7.19.0	All	All	All
Application	Haxx	Curl	7.19.1	All	All	All
Application	Haxx	Curl	7.19.2	All	All	All
Application	Haxx	Curl	7.19.3	All	All	All
Application	Haxx	Curl	7.19.4	All	All	All

Application	Haxx	Curl	7.19.5	All	All	All
Application	Haxx	Curl	7.19.6	All	All	All
Application	Haxx	Curl	7.19.7	All	All	All
Application	Haxx	Curl	7.20.0	All	All	All
Application	Haxx	Curl	7.20.1	All	All	All
Application	Haxx	Curl	7.21.0	All	All	All
Application	Haxx	Curl	7.21.1	All	All	All
Application	Haxx	Curl	7.21.2	All	All	All
Application	Haxx	Curl	7.21.3	All	All	All
Application	Haxx	Curl	7.21.4	All	All	All
Application	Haxx	Curl	7.21.5	All	All	All
Application	Haxx	Curl	7.21.6	All	All	All
Application	Haxx	Curl	7.21.7	All	All	All
Application	Haxx	Curl	7.22.0	All	All	All
Application	Haxx	Curl	7.23.0	All	All	All
Application	Haxx	Curl	7.23.1	All	All	All
Application	Haxx	Curl	7.24.0	All	All	All
Application	Haxx	Curl	7.25.0	All	All	All
Application	Haxx	Curl	7.26.0	All	All	All
Application	Haxx	Curl	7.27.0	All	All	All
Application	Haxx	Curl	7.28.0	All	All	All
Application	Haxx	Curl	7.28.1	All	All	All
Application	Haxx	Curl	7.29.0	All	All	All
Application	Haxx	Curl	7.30.0	All	All	All
Application	Haxx	Curl	7.31.0	All	All	All
Application	Haxx	Curl	7.32.0	All	All	All
Application	Haxx	Curl	7.33.0	All	All	All
Application	Haxx	Curl	7.34.0	All	All	All
Application	Haxx	Curl	7.35.0	All	All	All
Application	Haxx	Libcurl	7.10.6	All	All	All
Application	Haxx	Libcurl	7.10.7	All	All	All
Application	Haxx	Libcurl	7.10.8	All	All	All
Application	Haxx	Libcurl	7.11.0	All	All	All
Application	Haxx	Libcurl	7.11.1	All	All	All
Application	Haxx	Libcurl	7.11.2	All	All	All

Application	Haxx	Libcurl	7.12.0	All	All	All
Application	Haxx	Libcurl	7.12.1	All	All	All
Application	Haxx	Libcurl	7.12.2	All	All	All
Application	Haxx	Libcurl	7.12.3	All	All	All
Application	Haxx	Libcurl	7.13.0	All	All	All
Application	Haxx	Libcurl	7.13.1	All	All	All
Application	Haxx	Libcurl	7.13.2	All	All	All
Application	Haxx	Libcurl	7.14.0	All	All	All
Application	Haxx	Libcurl	7.14.1	All	All	All
Application	Haxx	Libcurl	7.15.0	All	All	All
Application	Haxx	Libcurl	7.15.1	All	All	All
Application	Haxx	Libcurl	7.15.2	All	All	All
Application	Haxx	Libcurl	7.15.3	All	All	All
Application	Haxx	Libcurl	7.15.4	All	All	All
Application	Haxx	Libcurl	7.15.5	All	All	All
Application	Haxx	Libcurl	7.16.0	All	All	All
Application	Haxx	Libcurl	7.16.1	All	All	All
Application	Haxx	Libcurl	7.16.2	All	All	All
Application	Haxx	Libcurl	7.16.3	All	All	All
Application	Haxx	Libcurl	7.16.4	All	All	All
Application	Haxx	Libcurl	7.17.0	All	All	All
Application	Haxx	Libcurl	7.17.1	All	All	All
Application	Haxx	Libcurl	7.18.0	All	All	All
Application	Haxx	Libcurl	7.18.1	All	All	All
Application	Haxx	Libcurl	7.18.2	All	All	All
Application	Haxx	Libcurl	7.19.0	All	All	All
Application	Haxx	Libcurl	7.19.1	All	All	All
Application	Haxx	Libcurl	7.19.2	All	All	All
Application	Haxx	Libcurl	7.19.3	All	All	All
Application	Haxx	Libcurl	7.19.4	All	All	All
Application	Haxx	Libcurl	7.19.5	All	All	All
Application	Haxx	Libcurl	7.19.6	All	All	All
Application	Haxx	Libcurl	7.19.7	All	All	All
Application	Haxx	Libcurl	7.20.0	All	All	All
Application	Haxx	Libcurl	7.20.1	All	All	All
Application	Haxx	Libcurl	7.20.2	All	All	All

Application	Haxx	Libcurl	7.21.0	All	All	All
Application	Haxx	Libcurl	7.21.1	All	All	All
Application	Haxx	Libcurl	7.21.2	All	All	All
Application	Haxx	Libcurl	7.21.3	All	All	All
Application	Haxx	Libcurl	7.21.4	All	All	All
Application	Haxx	Libcurl	7.21.5	All	All	All
Application	Haxx	Libcurl	7.21.6	All	All	All
Application	Haxx	Libcurl	7.21.7	All	All	All
Application	Haxx	Libcurl	7.22.0	All	All	All
Application	Haxx	Libcurl	7.23.0	All	All	All
Application	Haxx	Libcurl	7.23.1	All	All	All
Application	Haxx	Libcurl	7.24.0	All	All	All
Application	Haxx	Libcurl	7.25.0	All	All	All
Application	Haxx	Libcurl	7.26.0	All	All	All
Application	Haxx	Libcurl	7.27.0	All	All	All
Application	Haxx	Libcurl	7.28.0	All	All	All
Application	Haxx	Libcurl	7.28.1	All	All	All
Application	Haxx	Libcurl	7.29.0	All	All	All
Application	Haxx	Libcurl	7.30.0	All	All	All
Application	Haxx	Libcurl	7.31.0	All	All	All
Application	Haxx	Libcurl	7.32.0	All	All	All
Application	Haxx	Libcurl	7.33.0	All	All	All
Application	Haxx	Libcurl	7.34.0	All	All	All
Application	Haxx	Libcurl	7.35.0	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		

References
Reference
About Secunia Research Flexera
Enterprise Chef 11.1.3 Release Chef Blog
Oracle Critical Patch Update - July 2015
About Secunia Research Flexera
SecurityFocus
cURL - libcurl wrong re-use of connections

CVE - libcurl wrong re-use of connections

Debian -- Security Information -- DSA-2902-1 curl

openSUSE-SU-2014:0530-1: moderate: update for curl

Security Advisory SA58615 - IBM Tivoli Netcool System Service Monitors Multiple Security Issues and Multiple Vulnerabilities - Secunia

Security Bulletin: IBM Tivoli Netcool System Service Monitors/Application Service Monitors is affected by the following libcurl vulnerabilities:

Chef Server 11.0.12 Release | Chef Blog

IBM Support

USN-2167-1: curl vulnerabilities | Ubuntu

About Secunia Research | Flexera

Security Advisory SA59458 - IBM Multiple Products cURL Multiple Security Issues - Secunia

Enterprise Chef 1.4.9 Release | Chef Blog

Full Disclosure: NEW: VMSA-2014-0012 - VMware vSphere product updates address security vulnerabilities

VMSA-2014-0012 | United States

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[500110](#) Alpine Linux Security Update for curl

[503765](#) Alpine Linux Security Update for curl

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)