



# CVE-2018-1000301

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2018-1000301  |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | cve@mitre.org   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2018-05-24 13:29:00 UTC   |
| <b>Updated</b>         | 2019-10-03 00:03:00 UTC   |
| <b>Description</b>     | curl version curl 7.20.0 to and including curl 7.59.0 contains a CWE-126: Buffer Over-read vulnerability in denial of service t |

## Risk And Classification

**Problem Types:** CWE-125

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                    | Product                      | Version | Update | Edition | Language |
|------------------|---------------------------|------------------------------|---------|--------|---------|----------|
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 12.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 14.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 16.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 17.10   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 18.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 12.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 14.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 16.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 17.10   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 18.04   | All    | All     | All      |
| Operating System | <a href="#">Debian</a>    | <a href="#">Debian Linux</a> | 7.0     | All    | All     | All      |
| Operating System | <a href="#">Debian</a>    | <a href="#">Debian Linux</a> | 8.0     | All    | All     | All      |
| Operating System | <a href="#">Debian</a>    | <a href="#">Debian Linux</a> | 9.0     | All    | All     | All      |
| Operating System | <a href="#">Debian</a>    | <a href="#">Debian Linux</a> | 7.0     | All    | All     | All      |
| Operating System | <a href="#">Debian</a>    | <a href="#">Debian Linux</a> | 8.0     | All    | All     | All      |
| Operating System | <a href="#">Debian</a>    | <a href="#">Debian Linux</a> | 9.0     | All    | All     | All      |
| Application      | <a href="#">Haxx</a>      | <a href="#">Curl</a>         | All     | All    | All     | All      |

|                  |        |  |        |     |     |     |
|------------------|--------|--|--------|-----|-----|-----|
| Application      | Oracle | Communications WebRTC Session Controller | All    | All | All | All |
| Application      | Oracle | Communications WebRTC Session Controller | All    | All | All | All |
| Application      | Oracle | Enterprise Manager Ops Center            | 12.2.2 | All | All | All |
| Application      | Oracle | Enterprise Manager Ops Center            | 12.3.3 | All | All | All |
| Application      | Oracle | Enterprise Manager Ops Center            | 12.2.2 | All | All | All |
| Application      | Oracle | Enterprise Manager Ops Center            | 12.3.3 | All | All | All |
| Application      | Oracle | Peoplesoft Enterprise Peopletools        | 8.55   | All | All | All |
| Application      | Oracle | Peoplesoft Enterprise Peopletools        | 8.56   | All | All | All |
| Application      | Oracle | Peoplesoft Enterprise Peopletools        | 8.57   | All | All | All |
| Application      | Oracle | Peoplesoft Enterprise Peopletools        | 8.55   | All | All | All |
| Application      | Oracle | Peoplesoft Enterprise Peopletools        | 8.56   | All | All | All |
| Application      | Oracle | Peoplesoft Enterprise Peopletools        | 8.57   | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop                 | 7.0    | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop                 | 7.0    | All | All | All |
| Operating System | Redhat | Enterprise Linux Server                  | 7.0    | All | All | All |
| Operating System | Redhat | Enterprise Linux Server                  | 7.0    | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation             | 7.0    | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation             | 7.0    | All | All | All |

## References

### Reference

curl - RTSP bad headers buffer over-read - CVE-2018-1000301

Red Hat Customer Portal

CPU July 2018

Oracle Critical Patch Update - January 2019

Oracle Critical Patch Update - July 2019

cURL CVE-2018-1000301 Information Disclosure Vulnerability

curl RTSP Response Processing Flaw in Curl\_http\_readwrite\_headers() Lets Remote Users Deny Service or Obtain Potentially Sensitive Information

Red Hat Customer Portal

Red Hat Customer Portal

USN-3648-1: curl vulnerabilities | Ubuntu security notices

USN-3598-2: curl vulnerabilities | Ubuntu security notices

CPU Oct 2018

Red Hat Customer Portal

Debian -- Security Information -- DSA-4202-1 curl

SECURITY: DSA-4202-1: curl

cURL: Multiple vulnerabilities (GLSA 201806-05) — Gentoo Security

Red Hat Customer Portal

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[500123](#) Alpine Linux Security Update for curl

[503778](#) Alpine Linux Security Update for curl

[690572](#) Free Berkeley Software Distribution (FreeBSD) Security Update for curl (04fe6c8d-2a34-4009-a81e-e7a7e759b5d2)

[710308](#) Gentoo Linux cURL Multiple Vulnerabilities (GLSA 201806-05)

© [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](#)**