



# CVE-2015-3145

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

## Summary

|                 |                                                                                                                             |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2015-3145                                                                                                               |
| State           | PUBLISHED                                                                                                                   |
| Assigner        | redhat                                                                                                                      |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                                |
| Published       | 2015-04-24 14:59:10 UTC                                                                                                     |
| Updated         | 2026-05-06 22:30:45 UTC                                                                                                     |
| Description     | The sanitize_cookie_path function in cURL and libcurl 7.31.0 through 7.41.0 does not properly calculate an index, which all |

## Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

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

Problem Types: CWE-119 | n/a

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor | Product  | Version | Update | Edition | Language |
|------------------|--------|----------|---------|--------|---------|----------|
| Operating System | Apple  | Mac Os X | 10.10.0 | All    | All     | All      |

|                  |                               |                              |         |     |     |     |
|------------------|-------------------------------|------------------------------|---------|-----|-----|-----|
| Operating System | <a href="#">Apple</a>         | <a href="#">Mac Os X</a>     | 10.10.1 | All | All | All |
| Operating System | <a href="#">Apple</a>         | <a href="#">Mac Os X</a>     | 10.10.2 | All | All | All |
| Operating System | <a href="#">Apple</a>         | <a href="#">Mac Os X</a>     | 10.10.3 | All | All | All |
| Operating System | <a href="#">Apple</a>         | <a href="#">Mac Os X</a>     | 10.10.4 | 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> | 14.10   | All | All | All |
| Operating System | <a href="#">Canonical</a>     | <a href="#">Ubuntu Linux</a> | 15.04   | All | All | All |
| Operating System | <a href="#">Debian</a>        | <a href="#">Debian Linux</a> | 7.0     | All | All | All |
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>       | 21      | All | All | All |
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>       | 22      | All | All | All |
| Application      | <a href="#">Haxx</a>          | <a href="#">Curl</a>         | 7.31.0  | All | All | All |
| Application      | <a href="#">Haxx</a>          | <a href="#">Curl</a>         | 7.32.0  | All | All | All |
| Application      | <a href="#">Haxx</a>          | <a href="#">Curl</a>         | 7.33.0  | All | All | All |
| Application      | <a href="#">Haxx</a>          | <a href="#">Curl</a>         | 7.34.0  | All | All | All |
| Application      | <a href="#">Haxx</a>          | <a href="#">Curl</a>         | 7.35.0  | All | All | All |
| Application      | <a href="#">Haxx</a>          | <a href="#">Curl</a>         | 7.36.0  | All | All | All |
| Application      | <a href="#">Haxx</a>          | <a href="#">Curl</a>         | 7.37.0  | All | All | All |
| Application      | <a href="#">Haxx</a>          | <a href="#">Curl</a>         | 7.37.1  | All | All | All |
| Application      | <a href="#">Haxx</a>          | <a href="#">Curl</a>         | 7.38.0  | All | All | All |
| Application      | <a href="#">Haxx</a>          | <a href="#">Curl</a>         | 7.39.0  | All | All | All |
| Application      | <a href="#">Haxx</a>          | <a href="#">Curl</a>         | 7.40.0  | All | All | All |
| Application      | <a href="#">Haxx</a>          | <a href="#">Curl</a>         | 7.41.0  | All | All | All |
| Application      | <a href="#">Haxx</a>          | <a href="#">Libcurl</a>      | 7.30.0  | All | All | All |
| Application      | <a href="#">Haxx</a>          | <a href="#">Libcurl</a>      | 7.31.0  | All | All | All |
| Application      | <a href="#">Haxx</a>          | <a href="#">Libcurl</a>      | 7.32.0  | All | All | All |
| Application      | <a href="#">Haxx</a>          | <a href="#">Libcurl</a>      | 7.33.0  | All | All | All |
| Application      | <a href="#">Haxx</a>          | <a href="#">Libcurl</a>      | 7.34.0  | All | All | All |
| Application      | <a href="#">Haxx</a>          | <a href="#">Libcurl</a>      | 7.35.0  | All | All | All |
| Application      | <a href="#">Haxx</a>          | <a href="#">Libcurl</a>      | 7.36.0  | All | All | All |
| Application      | <a href="#">Haxx</a>          | <a href="#">Libcurl</a>      | 7.37.0  | All | All | All |
| Application      | <a href="#">Haxx</a>          | <a href="#">Libcurl</a>      | 7.37.1  | All | All | All |
| Application      | <a href="#">Haxx</a>          | <a href="#">Libcurl</a>      | 7.38.0  | All | All | All |
| Application      | <a href="#">Haxx</a>          | <a href="#">Libcurl</a>      | 7.39    | All | All | All |
| Application      | <a href="#">Haxx</a>          | <a href="#">Libcurl</a>      | 7.40.0  | All | All | All |
| Application      | <a href="#">Haxx</a>          | <a href="#">Libcurl</a>      | 7.41.0  | All | All | All |

|                  |                          |                                            |      |     |     |     |
|------------------|--------------------------|--------------------------------------------|------|-----|-----|-----|
| Application      | <a href="#">Hp</a>       | <a href="#">System Management Homepage</a> | All  | All | All | All |
| Operating System | <a href="#">Opensuse</a> | <a href="#">Opensuse</a>                   | 13.1 | All | All | All |
| Operating System | <a href="#">Opensuse</a> | <a href="#">Opensuse</a>                   | 13.2 | All | All | All |
| Operating System | <a href="#">Oracle</a>   | <a href="#">Solaris</a>                    | 11.3 | All | All | All |

| Vendor Declared Affected Products |                    |                     |              |               |  |  |
|-----------------------------------|--------------------|---------------------|--------------|---------------|--|--|
| Source                            | Vendor             | Product             | Version      | Platforms     |  |  |
| CNA                               | <a href="#">Na</a> | <a href="#">N/a</a> | affected n/a | Not specified |  |  |

| References                                                                                        |                                  |
|---------------------------------------------------------------------------------------------------|----------------------------------|
| Reference                                                                                         | Source                           |
| Document Display   HPE Support Center                                                             | af854a3a-2127-422b-91ae-364da26f |
| CPU Oct 2018                                                                                      | af854a3a-2127-422b-91ae-364da26f |
| libcurl Bugs Let Remote Users Deny Service and Execute Arbitrary Code - SecurityTracker           | af854a3a-2127-422b-91ae-364da26f |
| APPLE-SA-2015-08-13-2 OS X Yosemite v10.10.5 and Security Update 2015-006                         | af854a3a-2127-422b-91ae-364da26f |
| [SECURITY] Fedora 21 Update: mingw-curl-7.42.0-1.fc21                                             | af854a3a-2127-422b-91ae-364da26f |
| About the security content of OS X Yosemite v10.10.5 and Security Update 2015-006 - Apple Support | af854a3a-2127-422b-91ae-364da26f |
| USN-2591-1: curl vulnerabilities   Ubuntu                                                         | af854a3a-2127-422b-91ae-364da26f |
| cURL/libcURL CVE-2015-3145 Out of Bounds Read Denial of Service Vulnerability                     | af854a3a-2127-422b-91ae-364da26f |
| 2016-04 Security Bulletin: Junos: Multiple vulnerabilities in cURL and libcurl - Juniper Networks | af854a3a-2127-422b-91ae-364da26f |
| [SECURITY] Fedora 22 Update: curl-7.40.0-3.fc22                                                   | af854a3a-2127-422b-91ae-364da26f |
| Oracle Solaris Bulletin - January 2016                                                            | af854a3a-2127-422b-91ae-364da26f |
| [SECURITY] Fedora 20 Update: curl-7.32.0-20.fc20                                                  | af854a3a-2127-422b-91ae-364da26f |
| Gentoo Security                                                                                   | af854a3a-2127-422b-91ae-364da26f |
| openSUSE-SU-2015:0799-1: moderate: Security update for curl                                       | af854a3a-2127-422b-91ae-364da26f |
| [SECURITY] Fedora 21 Update: curl-7.37.0-14.fc21                                                  | af854a3a-2127-422b-91ae-364da26f |
| cURL - cookie parser out of boundary memory access                                                | af854a3a-2127-422b-91ae-364da26f |
| [SECURITY] Fedora 22 Update: mingw-curl-7.42.0-1.fc22                                             | af854a3a-2127-422b-91ae-364da26f |
| Mageia Advisory: MGASA-2015-0179 - Updated curl packages fix security vulnerabilities             | af854a3a-2127-422b-91ae-364da26f |
| Debian -- Security Information -- DSA-3232-1 curl                                                 | af854a3a-2127-422b-91ae-364da26f |
| Support / Security / Advisories // MDVSA-2015:219   Mandriva                                      | af854a3a-2127-422b-91ae-364da26f |
| CVE Program record                                                                                | CVE.ORG                          |
| NVD vulnerability detail                                                                          | NVD                              |

No vendor comments have been submitted for this CVE.

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

© [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](#)