



# CVE-2015-0807

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

## Summary

|                        |                                                                                                                         |
|------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2015-0807                                                                                                           |
| <b>State</b>           | PUBLIC                                                                                                                  |
| <b>Assigner</b>        | security@mozilla.org                                                                                                    |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                            |
| <b>Published</b>       | 2015-04-01 10:59:00 UTC                                                                                                 |
| <b>Updated</b>         | 2017-01-03 02:59:00 UTC                                                                                                 |
| <b>Description</b>     | The navigator.sendBeacon implementation in Mozilla Firefox before 37.0, Firefox ESR 31.x before 31.6, and Thunderbird b |

## Risk And Classification

### Problem Types: CWE-352

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                  | Product                     | Version | Update | Edition | Language |
|-------------|-------------------------|-----------------------------|---------|--------|---------|----------|
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox</a>     | All     | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 31.0    | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 31.1    | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 31.1.0  | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 31.1.1  | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 31.2    | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 31.3    | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 31.3.0  | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 31.4    | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 31.5    | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 31.5.1  | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 31.5.2  | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 31.5.3  | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 31.0    | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 31.1    | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 31.1.0  | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 31.1.1  | All    | All     | All      |

|             |                         |                             |        |     |     |     |
|-------------|-------------------------|-----------------------------|--------|-----|-----|-----|
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 31.2   | All | All | All |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 31.3   | All | All | All |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 31.3.0 | All | All | All |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 31.4   | All | All | All |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 31.5   | All | All | All |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 31.5.1 | All | All | All |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 31.5.2 | All | All | All |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 31.5.3 | All | All | All |
| Application | <a href="#">Mozilla</a> | <a href="#">Thunderbird</a> | All    | All | All | All |

| References                                                                                                                                   |
|----------------------------------------------------------------------------------------------------------------------------------------------|
| Reference                                                                                                                                    |
| 1111834 – (CVE-2015-0807) CORS request after preflight should not follow 30x redirect                                                        |
| Debian -- Security Information -- DSA-3212-1 icedove                                                                                         |
| [security-announce] openSUSE-SU-2015:1266-1: important: Mozilla (Firefox                                                                     |
| [security-announce] openSUSE-SU-2015:0892-1: important: Update to Firefo                                                                     |
| [security-announce] SUSE-SU-2015:0704-1: important: Security update for                                                                      |
| Mozilla Thunderbird Flaws Let Remote Users Execute Arbitrary Code and Conduct Cross-Site Request Forgery Attacks - SecurityTracker           |
| USN-2550-1: Firefox vulnerabilities   Ubuntu                                                                                                 |
| CORS requests should not follow 30x redirections after preflight — Mozilla                                                                   |
| Red Hat Customer Portal                                                                                                                      |
| Mozilla Firefox Bugs Let Remote Users Execute Arbitrary Code, Bypass Security Restrictions, and Obtain Potentially Sensitive Information - S |
| Mozilla Products: Multiple vulnerabilities (GLSA 201512-10) — Gentoo Security                                                                |
| USN-2552-1: Thunderbird vulnerabilities   Ubuntu                                                                                             |
| Debian -- Security Information -- DSA-3211-1 iceweasel                                                                                       |
| Mozilla Firefox/Thunderbird 'sendBeacon()' Function Cross-Site Request Forgery Vulnerability                                                 |
| Oracle Solaris Third Party Bulletin - April 2015                                                                                             |
| [security-announce] openSUSE-SU-2015:0677-1: important: Security update                                                                      |
| Red Hat Customer Portal                                                                                                                      |
| CVE Program record                                                                                                                           |
| NVD vulnerability detail                                                                                                                     |
| ◀                                                                                                                                            |
| ▶                                                                                                                                            |

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](#)