



# CVE-2014-1556

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

## Summary

|                        |                                                                                                                            |
|------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2014-1556                                                                                                              |
| <b>State</b>           | PUBLIC                                                                                                                     |
| <b>Assigner</b>        | security@mozilla.org                                                                                                       |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                               |
| <b>Published</b>       | 2014-07-23 11:12:00 UTC                                                                                                    |
| <b>Updated</b>         | 2017-01-07 02:59:00 UTC                                                                                                    |
| <b>Description</b>     | Mozilla Firefox before 31.0, Firefox ESR 24.x before 24.7, and Thunderbird before 24.7 allow remote attackers to execute a |

## Risk And Classification

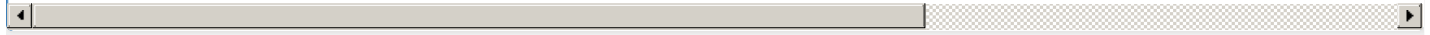
### Problem Types: CWE-94

## 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> | 24.0    | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 24.0.1  | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 24.0.2  | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 24.1.0  | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 24.1.1  | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 24.2    | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 24.3    | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 24.4    | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 24.5    | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 24.6    | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 24.0    | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 24.0.1  | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 24.0.2  | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 24.1.0  | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 24.1.1  | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 24.2    | All    | All     | All      |

|             |                         |                             |        |     |     |     |
|-------------|-------------------------|-----------------------------|--------|-----|-----|-----|
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 24.3   | All | All | All |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 24.4   | All | All | All |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 24.5   | All | All | All |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 24.6   | All | All | All |
| Application | <a href="#">Mozilla</a> | <a href="#">Thunderbird</a> | 24.0   | All | All | All |
| Application | <a href="#">Mozilla</a> | <a href="#">Thunderbird</a> | 24.0.1 | All | All | All |
| Application | <a href="#">Mozilla</a> | <a href="#">Thunderbird</a> | 24.1   | All | All | All |
| Application | <a href="#">Mozilla</a> | <a href="#">Thunderbird</a> | 24.1.1 | All | All | All |
| Application | <a href="#">Mozilla</a> | <a href="#">Thunderbird</a> | 24.2   | All | All | All |
| Application | <a href="#">Mozilla</a> | <a href="#">Thunderbird</a> | 24.3   | All | All | All |
| Application | <a href="#">Mozilla</a> | <a href="#">Thunderbird</a> | 24.4   | All | All | All |
| Application | <a href="#">Mozilla</a> | <a href="#">Thunderbird</a> | 24.5   | All | All | All |
| Application | <a href="#">Mozilla</a> | <a href="#">Thunderbird</a> | 24.0   | All | All | All |
| Application | <a href="#">Mozilla</a> | <a href="#">Thunderbird</a> | 24.0.1 | All | All | All |
| Application | <a href="#">Mozilla</a> | <a href="#">Thunderbird</a> | 24.1   | All | All | All |
| Application | <a href="#">Mozilla</a> | <a href="#">Thunderbird</a> | 24.1.1 | All | All | All |
| Application | <a href="#">Mozilla</a> | <a href="#">Thunderbird</a> | 24.2   | All | All | All |
| Application | <a href="#">Mozilla</a> | <a href="#">Thunderbird</a> | 24.3   | All | All | All |
| Application | <a href="#">Mozilla</a> | <a href="#">Thunderbird</a> | 24.4   | All | All | All |
| Application | <a href="#">Mozilla</a> | <a href="#">Thunderbird</a> | 24.5   | All | All | All |
| Application | <a href="#">Mozilla</a> | <a href="#">Thunderbird</a> | All    | All | All | All |

| References                                                                      |
|---------------------------------------------------------------------------------|
| <b>Reference</b>                                                                |
| Security Advisory SA60628 - SUSE update for MozillaFirefox - Secunia            |
| Oracle Solaris Bulletin - April 2016                                            |
| About Secunia Research   Flexera                                                |
| Mozilla Firefox/Thunderbird CVE-2014-1556 Remote Code Execution Vulnerability   |
| Access Denied                                                                   |
| Gentoo Security                                                                 |
| linux.oracle.com   ELSA-2014-0918                                               |
| About Secunia Research   Flexera                                                |
| MFSA 2014-62: Exploitable WebGL crash with Cesium JavaScript library            |
| Security Advisory SA59591 - Debian update for icedove - Secunia                 |
| Security Advisory SA59760 - Waterfox Firefox Multiple Vulnerabilities - Secunia |

|                                                                                                                                           |
|-------------------------------------------------------------------------------------------------------------------------------------------|
| Debian -- Security Information -- DSA-2996-1 icedove                                                                                      |
| Mozilla Thunderbird Multiple Flaws Let Remote Users Deny Service and Execute Arbitrary Code - SecurityTracker                             |
| Security Advisory SA59719 - SUSE update for MozillaFirefox - Secunia                                                                      |
| Security Advisory SA60621 - SUSE update for MozillaFirefox and MozillaThunderbird - Secunia                                               |
| Mozilla Firefox Multiple Flaws Let Remote Users Execute Arbitrary Code, Deny Service, and Spoof User Interface Elements - SecurityTracker |
| Security Advisory SA60083 - SUSE update for MozillaThunderbird - Secunia                                                                  |
| Debian -- Security Information -- DSA-2986-1 iceweasel                                                                                    |
| 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.                                                                      |