



# CVE-2017-5400

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

## Summary

|                        |                                                                                                                          |
|------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2017-5400                                                                                                            |
| <b>State</b>           | PUBLIC                                                                                                                   |
| <b>Assigner</b>        | security@mozilla.org                                                                                                     |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                             |
| <b>Published</b>       | 2018-06-11 21:29:00 UTC                                                                                                  |
| <b>Updated</b>         | 2018-08-07 12:56:00 UTC                                                                                                  |
| <b>Description</b>     | JIT-spray targeting asm.js combined with a heap spray allows for a bypass of ASLR and DEP protections leading to potenti |

## Risk And Classification

### Problem Types: CWE-119

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                  | Product                                  | Version | Update | Edition | Language |
|------------------|-------------------------|------------------------------------------|---------|--------|---------|----------|
| 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>             | 8.0     | All    | All     | All      |
| Application      | <a href="#">Mozilla</a> | <a href="#">Firefox</a>                  | All     | All    | All     | All      |
| Application      | <a href="#">Mozilla</a> | <a href="#">Firefox</a>                  | All     | All    | All     | All      |
| Application      | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a>              | All     | All    | All     | All      |
| Application      | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a>              | All     | All    | All     | All      |
| Application      | <a href="#">Mozilla</a> | <a href="#">Thunderbird</a>              | All     | All    | All     | All      |
| Application      | <a href="#">Mozilla</a> | <a href="#">Thunderbird</a>              | All     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a>  | <a href="#">Enterprise Linux Desktop</a> | 5.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a>  | <a href="#">Enterprise Linux Desktop</a> | 6.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a>  | <a href="#">Enterprise Linux Desktop</a> | 7.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a>  | <a href="#">Enterprise Linux Desktop</a> | 5.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a>  | <a href="#">Enterprise Linux Desktop</a> | 6.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a>  | <a href="#">Enterprise Linux Desktop</a> | 7.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a>  | <a href="#">Enterprise Linux Server</a>  | 5.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a>  | <a href="#">Enterprise Linux Server</a>  | 6.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a>  | <a href="#">Enterprise Linux Server</a>  | 7.0     | All    | All     | All      |

|                  |                        |                                              |     |     |     |     |
|------------------|------------------------|----------------------------------------------|-----|-----|-----|-----|
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server</a>      | 5.0 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server</a>      | 6.0 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server</a>      | 7.0 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server Aus</a>  | 7.3 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server Aus</a>  | 7.4 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server Aus</a>  | 7.3 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server Aus</a>  | 7.4 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server Eus</a>  | 7.3 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server Eus</a>  | 7.4 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server Eus</a>  | 7.5 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server Eus</a>  | 7.3 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server Eus</a>  | 7.4 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server Eus</a>  | 7.5 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Workstation</a> | 5.0 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Workstation</a> | 6.0 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Workstation</a> | 7.0 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Workstation</a> | 5.0 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Workstation</a> | 6.0 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Workstation</a> | 7.0 | All | All | All |

References

Reference

Mozilla Thunderbird: Multiple vulnerabilities (GLSA 201705-07) — Gentoo Security

Red Hat Customer Portal

Security vulnerabilities fixed in Thunderbird 45.8 — Mozilla

Mozilla Firefox: Multiple vulnerabilities (GLSA 201705-06) — Gentoo security

Mozilla Firefox Multiple Bugs Let Remote Users Bypass Security Restrictions, Spoof URLs, Obtain Potentially Sensitive Information, Deny Ser

Debian -- Security Information -- DSA-3832-1 icedove

Security vulnerabilities fixed in - Thunderbird 52 — Mozilla

Red Hat Customer Portal

Security vulnerabilities fixed in Firefox ESR 45.8 — Mozilla

Mozilla Firefox and Thunderbird CVE-2017-5400 Multiple Memory-Corruption Vulnerabilities

Access Denied

Red Hat Customer Portal

Debian -- Security Information -- DSA-3805-1 firefox-esr

[CVE Program record](#)

[NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[378239](#) Virtuozzo Linux Security Update for thunderbird (VZLSA-2017:0498)

[378313](#) Virtuozzo Linux Security Update for firefox (VZLSA-2017:0459)

[378319](#) Virtuozzo Linux Security Update for firefox (VZLSA-2017:0461)

[710423](#) Gentoo Linux Mozilla Firefox Multiple Vulnerabilities (GLSA 201705-06)

[710543](#) Gentoo Linux Mozilla Thunderbird Multiple Vulnerabilities (GLSA 201705-07)

© [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](#)