



# CVE-2013-0771

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

## Summary

|                        |                                                                                                                           |
|------------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2013-0771                                                                                                             |
| <b>State</b>           | PUBLIC                                                                                                                    |
| <b>Assigner</b>        | security@mozilla.org                                                                                                      |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                              |
| <b>Published</b>       | 2013-01-13 20:55:00 UTC                                                                                                   |
| <b>Updated</b>         | 2020-08-11 13:14:00 UTC                                                                                                   |
| <b>Description</b>     | Heap-based buffer overflow in the gfxTextRun::ShrinkToLigatureBoundaries function in Mozilla Firefox before 18.0, Firefox |

## Risk And Classification

### Problem Types: CWE-787

## 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>    | 10.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a>    | 11.10   | 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>    | 12.10   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a>    | 10.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a>    | 11.10   | 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>    | 12.10   | 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="#">Seamonkey</a>       | All     | All    | All     | All      |
| Application      | <a href="#">Mozilla</a>   | <a href="#">Seamonkey</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      |
| Application      | <a href="#">Mozilla</a>   | <a href="#">Thunderbird Esr</a> | All     | All    | All     | All      |

|                  |                          |                                                           |      |     |     |     |
|------------------|--------------------------|-----------------------------------------------------------|------|-----|-----|-----|
| Application      | <a href="#">Mozilla</a>  | <a href="#">Thunderbird Esr</a>                           | All  | All | All | All |
| Operating System | <a href="#">Opensuse</a> | <a href="#">Opensuse</a>                                  | 11.4 | All | All | All |
| Operating System | <a href="#">Opensuse</a> | <a href="#">Opensuse</a>                                  | 12.1 | All | All | All |
| Operating System | <a href="#">Opensuse</a> | <a href="#">Opensuse</a>                                  | 12.2 | All | All | All |
| Operating System | <a href="#">Opensuse</a> | <a href="#">Opensuse</a>                                  | 11.4 | All | All | All |
| Operating System | <a href="#">Opensuse</a> | <a href="#">Opensuse</a>                                  | 12.1 | All | All | All |
| Operating System | <a href="#">Opensuse</a> | <a href="#">Opensuse</a>                                  | 12.2 | All | All | All |
| Operating System | <a href="#">Suse</a>     | <a href="#">Linux Enterprise Desktop</a>                  | 10   | sp4 | All | All |
| Operating System | <a href="#">Suse</a>     | <a href="#">Linux Enterprise Desktop</a>                  | 11   | sp2 | All | All |
| Operating System | <a href="#">Suse</a>     | <a href="#">Linux Enterprise Desktop</a>                  | 10   | sp4 | All | All |
| Operating System | <a href="#">Suse</a>     | <a href="#">Linux Enterprise Desktop</a>                  | 11   | sp2 | All | All |
| Operating System | <a href="#">Suse</a>     | <a href="#">Linux Enterprise Server</a>                   | 10   | sp4 | All | All |
| Operating System | <a href="#">Suse</a>     | <a href="#">Linux Enterprise Server</a>                   | 11   | sp2 | All | All |
| Operating System | <a href="#">Suse</a>     | <a href="#">Linux Enterprise Server</a>                   | 11   | sp2 | All | All |
| Operating System | <a href="#">Suse</a>     | <a href="#">Linux Enterprise Server</a>                   | 10   | sp4 | All | All |
| Operating System | <a href="#">Suse</a>     | <a href="#">Linux Enterprise Server</a>                   | 11   | sp2 | All | All |
| Operating System | <a href="#">Suse</a>     | <a href="#">Linux Enterprise Server</a>                   | 11   | sp2 | All | All |
| Operating System | <a href="#">Suse</a>     | <a href="#">Linux Enterprise Software Development Kit</a> | 10   | sp4 | All | All |
| Operating System | <a href="#">Suse</a>     | <a href="#">Linux Enterprise Software Development Kit</a> | 11   | sp2 | All | All |
| Operating System | <a href="#">Suse</a>     | <a href="#">Linux Enterprise Software Development Kit</a> | 10   | sp4 | All | All |
| Operating System | <a href="#">Suse</a>     | <a href="#">Linux Enterprise Software Development Kit</a> | 11   | sp2 | All | All |

| References                                                                              |  |  |         |                                      |             |  |
|-----------------------------------------------------------------------------------------|--|--|---------|--------------------------------------|-------------|--|
| Reference                                                                               |  |  | Source  | Link                                 | Tags        |  |
| [security-announce] SUSE-SU-2013:0048-1: important: Security update for                 |  |  | SUSE    | <a href="#">lists.opensuse.org</a>   | Mailing Lis |  |
| MFSA 2013-02: Use-after-free and buffer overflow issues found using Address Sanitizer   |  |  | CONFIRM | <a href="#">www.mozilla.org</a>      | Vendor Ac   |  |
| 785555 – (CVE-2013-0771) Heap-buffer-overflow in gfxTextRun::ShrinkToLigatureBoundaries |  |  | CONFIRM | <a href="#">bugzilla.mozilla.org</a> | Issue Trac  |  |
| USN-1681-1: Firefox vulnerabilities   Ubuntu                                            |  |  | UBUNTU  | <a href="#">www.ubuntu.com</a>       | Third Part  |  |
| Repository / Oval Repository                                                            |  |  | OVAL    | <a href="#">oval.cisecurity.org</a>  | Third Part  |  |
| [security-announce] openSUSE-SU-2013:0131-1: important: Mozilla Januarys                |  |  | SUSE    | <a href="#">lists.opensuse.org</a>   | Mailing Lis |  |
| USN-1681-4: Firefox regression   Ubuntu                                                 |  |  | UBUNTU  | <a href="#">www.ubuntu.com</a>       | Third Part  |  |
| USN-1681-2: Thunderbird vulnerabilities   Ubuntu                                        |  |  | UBUNTU  | <a href="#">www.ubuntu.com</a>       | Third Part  |  |
| [security-announce] openSUSE-SU-2013:0149-1: important: Mozilla Januarys                |  |  | SUSE    | <a href="#">lists.opensuse.org</a>   | Mailing Lis |  |
| [security-announce] SUSE-SU-2013:0049-1: important: Security update for                 |  |  | SUSE    | <a href="#">lists.opensuse.org</a>   | Mailing Lis |  |
| CVE Program record                                                                      |  |  | CVE.ORG | <a href="#">www.cve.org</a>          | canonical   |  |

No vendor comments have been submitted for this CVE.

#### Legacy QID Mappings

[690332](#) Free Berkeley Software Distribution (FreeBSD) Security Update for mozilla (a4ed6632-5aa9-11e2-8fcb-c8600054b392)

© [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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)