



# CVE-2012-4214

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

## Summary

|                        |                                                                                                                                |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2012-4214                                                                                                                  |
| <b>State</b>           | PUBLIC                                                                                                                         |
| <b>Assigner</b>        | cve@mitre.org                                                                                                                  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                   |
| <b>Published</b>       | 2012-11-21 12:55:00 UTC                                                                                                        |
| <b>Updated</b>         | 2020-08-13 19:38:00 UTC                                                                                                        |
| <b>Description</b>     | Use-after-free vulnerability in the nsTextEditorState::PrepareEditor function in Mozilla Firefox before 17.0, Firefox ESR 10.x |

## Risk And Classification

### Problem Types: CWE-416

## 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      | Mozilla  | Thunderbird Esr                           | All  | All | All | All |
| Operating System | Opensuse | Opensuse                                  | 11.4 | All | All | All |
| Operating System | Opensuse | Opensuse                                  | 12.1 | All | All | All |
| Operating System | Opensuse | Opensuse                                  | 12.2 | All | All | All |
| Operating System | Opensuse | Opensuse                                  | 11.4 | All | All | All |
| Operating System | Opensuse | Opensuse                                  | 12.1 | All | All | All |
| Operating System | Opensuse | Opensuse                                  | 12.2 | All | All | All |
| Operating System | Redhat   | Enterprise Linux Desktop                  | 5.0  | All | All | All |
| Operating System | Redhat   | Enterprise Linux Desktop                  | 6.0  | All | All | All |
| Operating System | Redhat   | Enterprise Linux Desktop                  | 5.0  | All | All | All |
| Operating System | Redhat   | Enterprise Linux Desktop                  | 6.0  | All | All | All |
| Operating System | Redhat   | Enterprise Linux Eus                      | 6.3  | All | All | All |
| Operating System | Redhat   | Enterprise Linux Eus                      | 6.3  | All | All | All |
| Operating System | Redhat   | Enterprise Linux Server                   | 5.0  | All | All | All |
| Operating System | Redhat   | Enterprise Linux Server                   | 6.0  | All | All | All |
| Operating System | Redhat   | Enterprise Linux Server                   | 5.0  | All | All | All |
| Operating System | Redhat   | Enterprise Linux Server                   | 6.0  | All | All | All |
| Operating System | Redhat   | Enterprise Linux Workstation              | 5.0  | All | All | All |
| Operating System | Redhat   | Enterprise Linux Workstation              | 6.0  | All | All | All |
| Operating System | Redhat   | Enterprise Linux Workstation              | 5.0  | All | All | All |
| Operating System | Redhat   | Enterprise Linux Workstation              | 6.0  | All | All | All |
| Operating System | Suse     | Linux Enterprise Desktop                  | 10   | sp4 | All | All |
| Operating System | Suse     | Linux Enterprise Desktop                  | 11   | sp2 | All | All |
| Operating System | Suse     | Linux Enterprise Desktop                  | 10   | sp4 | All | All |
| Operating System | Suse     | Linux Enterprise Desktop                  | 11   | sp2 | All | All |
| Operating System | Suse     | Linux Enterprise Server                   | 10   | sp4 | All | All |
| Operating System | Suse     | Linux Enterprise Server                   | 11   | sp2 | All | All |
| Operating System | Suse     | Linux Enterprise Server                   | 11   | sp2 | All | All |
| Operating System | Suse     | Linux Enterprise Server                   | 10   | sp4 | All | All |
| Operating System | Suse     | Linux Enterprise Server                   | 11   | sp2 | All | All |
| Operating System | Suse     | Linux Enterprise Server                   | 11   | sp2 | All | All |
| Operating System | Suse     | Linux Enterprise Software Development Kit | 10   | sp4 | All | All |
| Operating System | Suse     | Linux Enterprise Software Development Kit | 11   | sp2 | All | All |
| Operating System | Suse     | Linux Enterprise Software Development Kit | 10   | sp4 | All | All |
| Operating System | Suse     | Linux Enterprise Software Development Kit | 11   | sp2 | All | All |

## References

| Reference                                                                                          | Source   | Link                                                                                                  |
|----------------------------------------------------------------------------------------------------|----------|-------------------------------------------------------------------------------------------------------|
| Mozilla Firefox/Thunderbird/SeaMonkey CVE-2012-4214 Use After Free Memory Corruption Vulnerability | BID      | <a href="http://www.securityfocus.com/bid/50804">www.securityfocus.com</a>                            |
| Security Advisory SA51440 - SUSE update for seamonkey - Secunia                                    | SECUNIA  | <a href="http://secunia.com/advisories/51440">secunia.com</a>                                         |
| Security Advisory SA51359 - Red Hat update for firefox - Secunia                                   | SECUNIA  | <a href="http://secunia.com/advisories/51359">secunia.com</a>                                         |
| Security Advisory SA51434 - SUSE update for xulrunner - Secunia                                    | SECUNIA  | <a href="http://secunia.com/advisories/51434">secunia.com</a>                                         |
| openSUSE-SU-2012:1583-1: moderate: update for MozillaFirefox                                       | SUSE     | <a href="http://lists.opensuse.org/2012/07/20/2012072015831.html">lists.opensuse.org</a>              |
| Red Hat Customer Portal                                                                            | REDHAT   | <a href="http://rhn.redhat.com/errata/rhn Errata for Red Hat Enterprise Linux 5">rhn.redhat.com</a>   |
| openSUSE-SU-2012:1585-1: moderate: update for MozillaThunderbird                                   | SUSE     | <a href="http://lists.opensuse.org/2012/07/20/2012072015851.html">lists.opensuse.org</a>              |
| USN-1636-1: Thunderbird vulnerabilities   Ubuntu                                                   | UBUNTU   | <a href="http://www.ubuntu.com/usn/USN-1636-1">www.ubuntu.com</a>                                     |
| Repository / Oval Repository                                                                       | OVAL     | <a href="http://oval.cisecurity.org/repository">oval.cisecurity.org</a>                               |
| USN-1638-2: ubufox update   Ubuntu                                                                 | UBUNTU   | <a href="http://www.ubuntu.com/usn/USN-1638-2">www.ubuntu.com</a>                                     |
| Security Advisory SA51360 - Red Hat update for thunderbird - Secunia                               | SECUNIA  | <a href="http://secunia.com/advisories/51360">secunia.com</a>                                         |
| Red Hat Customer Portal                                                                            | REDHAT   | <a href="http://rhn.redhat.com/errata/rhn Errata for Red Hat Enterprise Linux 5">rhn.redhat.com</a>   |
| 795804 – (CVE-2012-4214) Heap-use-after-free in nsTextEditorState::PrepareEditor                   | CONFIRM  | <a href="https://bugzilla.mozilla.org/show_bug.cgi?id=795804">bugzilla.mozilla.org</a>                |
| USN-1638-1: Firefox vulnerabilities   Ubuntu                                                       | UBUNTU   | <a href="http://www.ubuntu.com/usn/USN-1638-1">www.ubuntu.com</a>                                     |
| About Secunia Research   Flexera                                                                   | SECUNIA  | <a href="http://secunia.com/research">secunia.com</a>                                                 |
| MFSA 2012-105: Use-after-free and buffer overflow issues found using Address Sanitizer             | CONFIRM  | <a href="http://www.mozilla.org/security/announcements/mfsa2012-105">www.mozilla.org</a>              |
| Support / Security / Advisories // MDVSA-2012:173   Mandriva                                       | MANDRIVA | <a href="http://www.mandriva.com/en/Security/Advisories/MDVSA-2012:173">www.mandriva.com</a>          |
| IBM X-Force Exchange                                                                               | XF       | <a href="http://exchange.xforce.ibmcloud.com/vulnerabilities/795804">exchange.xforce.ibmcloud.com</a> |
| [security-announce] SUSE-SU-2012:1592-1: important: Security update for                            | SUSE     | <a href="http://lists.opensuse.org/2012/07/20/2012072015921.html">lists.opensuse.org</a>              |
| USN-1638-3: Firefox regressions   Ubuntu                                                           | UBUNTU   | <a href="http://www.ubuntu.com/usn/USN-1638-3">www.ubuntu.com</a>                                     |
| Pale Moon -                                                                                        | CONFIRM  | <a href="http://www.palemoon.org">www.palemoon.org</a>                                                |
| [security-announce] openSUSE-SU-2013:0175-1: important: security update                            | SUSE     | <a href="http://lists.opensuse.org/2013/01/17/2013011701751.html">lists.opensuse.org</a>              |
| Security Advisory SA51369 - Ubuntu update for firefox - Secunia                                    | SECUNIA  | <a href="http://secunia.com/advisories/51369">secunia.com</a>                                         |
| Security Advisory SA51370 - Ubuntu update for thunderbird - Secunia                                | SECUNIA  | <a href="http://secunia.com/advisories/51370">secunia.com</a>                                         |
| openSUSE-SU-2012:1586-1: moderate: update for xulrunner                                            | SUSE     | <a href="http://lists.opensuse.org/2012/07/20/2012072015861.html">lists.opensuse.org</a>              |
| Security Advisory SA51439 - SUSE update for MozillaFirefox - Secunia                               | SECUNIA  | <a href="http://secunia.com/advisories/51439">secunia.com</a>                                         |
| CVE Program record                                                                                 | CVE.ORG  | <a href="http://www.cve.org">www.cve.org</a>                                                          |
| NVD vulnerability detail                                                                           | NVD      | <a href="http://nvd.nist.gov">nvd.nist.gov</a>                                                        |

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](#)