



# CVE-2013-1685

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

## Summary

|                        |                                                                                                                             |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2013-1685                                                                                                               |
| <b>State</b>           | PUBLIC                                                                                                                      |
| <b>Assigner</b>        | security@mozilla.org                                                                                                        |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                |
| <b>Published</b>       | 2013-06-26 03:19:00 UTC                                                                                                     |
| <b>Updated</b>         | 2017-09-19 01:36:00 UTC                                                                                                     |
| <b>Description</b>     | Use-after-free vulnerability in the nsIDocument::GetRootElement function in Mozilla Firefox before 22.0, Firefox ESR 17.x b |

## Risk And Classification

### Problem Types: CWE-399

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                  | Product                     | Version | Update | Edition | Language |
|-------------|-------------------------|-----------------------------|---------|--------|---------|----------|
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox</a>     | 19.0    | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox</a>     | 19.0.1  | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox</a>     | 19.0.2  | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox</a>     | 20.0    | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox</a>     | 20.0.1  | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox</a>     | 19.0    | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox</a>     | 19.0.1  | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox</a>     | 19.0.2  | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox</a>     | 20.0    | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox</a>     | 20.0.1  | 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> | 17.0    | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 17.0.1  | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 17.0.2  | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 17.0.3  | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 17.0.4  | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox Esr</a> | 17.0.5  | All    | All     | All      |

|             |         |                 |        |     |     |     |
|-------------|---------|-----------------|--------|-----|-----|-----|
|             |         |                 |        |     |     |     |
| Application | Mozilla | Firefox Esr     | 17.0.6 | All | All | All |
| Application | Mozilla | Firefox Esr     | 17.0   | All | All | All |
| Application | Mozilla | Firefox Esr     | 17.0.1 | All | All | All |
| Application | Mozilla | Firefox Esr     | 17.0.2 | All | All | All |
| Application | Mozilla | Firefox Esr     | 17.0.3 | All | All | All |
| Application | Mozilla | Firefox Esr     | 17.0.4 | All | All | All |
| Application | Mozilla | Firefox Esr     | 17.0.5 | All | All | All |
| Application | Mozilla | Firefox Esr     | 17.0.6 | All | All | All |
| Application | Mozilla | Thunderbird     | 17.0   | All | All | All |
| Application | Mozilla | Thunderbird     | 17.0.1 | All | All | All |
| Application | Mozilla | Thunderbird     | 17.0.2 | All | All | All |
| Application | Mozilla | Thunderbird     | 17.0.3 | All | All | All |
| Application | Mozilla | Thunderbird     | 17.0.4 | All | All | All |
| Application | Mozilla | Thunderbird     | 17.0.5 | All | All | All |
| Application | Mozilla | Thunderbird     | 17.0   | All | All | All |
| Application | Mozilla | Thunderbird     | 17.0.1 | All | All | All |
| Application | Mozilla | Thunderbird     | 17.0.2 | All | All | All |
| Application | Mozilla | Thunderbird     | 17.0.3 | All | All | All |
| Application | Mozilla | Thunderbird     | 17.0.4 | All | All | All |
| Application | Mozilla | Thunderbird     | 17.0.5 | All | All | All |
| Application | Mozilla | Thunderbird     | All    | All | All | All |
| Application | Mozilla | Thunderbird Esr | 17.0   | All | All | All |
| Application | Mozilla | Thunderbird Esr | 17.0.1 | All | All | All |
| Application | Mozilla | Thunderbird Esr | 17.0.2 | All | All | All |
| Application | Mozilla | Thunderbird Esr | 17.0.3 | All | All | All |
| Application | Mozilla | Thunderbird Esr | 17.0.4 | All | All | All |
| Application | Mozilla | Thunderbird Esr | 17.0.5 | All | All | All |
| Application | Mozilla | Thunderbird Esr | 17.0.6 | All | All | All |
| Application | Mozilla | Thunderbird Esr | 17.0   | All | All | All |
| Application | Mozilla | Thunderbird Esr | 17.0.1 | All | All | All |
| Application | Mozilla | Thunderbird Esr | 17.0.2 | All | All | All |
| Application | Mozilla | Thunderbird Esr | 17.0.3 | All | All | All |
| Application | Mozilla | Thunderbird Esr | 17.0.4 | All | All | All |
| Application | Mozilla | Thunderbird Esr | 17.0.5 | All | All | All |
| Application | Mozilla | Thunderbird Esr | 17.0.6 | All | All | All |

## References

| Reference                                                                | Source  | Link                                                             | Tags                |
|--------------------------------------------------------------------------|---------|------------------------------------------------------------------|---------------------|
| Debian -- Security Information -- DSA-2720-1 icedove                     | DEBIAN  | <a href="http://www.debian.org">www.debian.org</a>               |                     |
| Debian -- Security Information -- DSA-2716-1 iceweasel                   | DEBIAN  | <a href="http://www.debian.org">www.debian.org</a>               |                     |
| [security-announce] openSUSE-SU-2013:1142-1: important: MozillaFirefox:  | SUSE    | <a href="http://lists.opensuse.org">lists.opensuse.org</a>       |                     |
| MFSA 2013-50: Memory corruption found using Address Sanitizer            | CONFIRM | <a href="http://www.mozilla.org">www.mozilla.org</a>             | Vendor Advisory     |
| Access Denied                                                            | CONFIRM | <a href="http://bugzilla.mozilla.org">bugzilla.mozilla.org</a>   |                     |
| Red Hat Customer Portal                                                  | REDHAT  | <a href="http://rhn.redhat.com">rhn.redhat.com</a>               |                     |
| [security-announce] SUSE-SU-2013:1153-1: important: Security update for  | SUSE    | <a href="http://lists.opensuse.org">lists.opensuse.org</a>       |                     |
| [security-announce] openSUSE-SU-2013:1143-1: important: xulrunner: 17.0. | SUSE    | <a href="http://lists.opensuse.org">lists.opensuse.org</a>       |                     |
| Malformed Request                                                        | BID     | <a href="http://www.securityfocus.com">www.securityfocus.com</a> |                     |
| USN-1891-1: Thunderbird vulnerabilities   Ubuntu                         | UBUNTU  | <a href="http://www.ubuntu.com">www.ubuntu.com</a>               |                     |
| Repository / Oval Repository                                             | OVAL    | <a href="http://oval.cisecurity.org">oval.cisecurity.org</a>     |                     |
| Red Hat Customer Portal                                                  | REDHAT  | <a href="http://rhn.redhat.com">rhn.redhat.com</a>               |                     |
| [security-announce] openSUSE-SU-2013:1141-1: important: MozillaThunderbi | SUSE    | <a href="http://lists.opensuse.org">lists.opensuse.org</a>       |                     |
| [security-announce] openSUSE-SU-2013:1140-1: important: regular updates  | SUSE    | <a href="http://lists.opensuse.org">lists.opensuse.org</a>       |                     |
| [security-announce] SUSE-SU-2013:1152-1: important: Security update for  | SUSE    | <a href="http://lists.opensuse.org">lists.opensuse.org</a>       |                     |
| USN-1890-1: Firefox vulnerabilities   Ubuntu                             | UBUNTU  | <a href="http://www.ubuntu.com">www.ubuntu.com</a>               |                     |
| CVE Program record                                                       | CVE.ORG | <a href="http://www.cve.org">www.cve.org</a>                     | canonical           |
| NVD vulnerability detail                                                 | NVD     | <a href="http://nvd.nist.gov">nvd.nist.gov</a>                   | canonical, analysis |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](http://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](http://The MITRE Corporation) and the authoritative source of CVE content is [MITRE's CVE web site](http://MITRE's CVE web site). This site includes MITRE data granted under the following [license](http://license).

**Free CVE JSON API** [cve.report/api](http://cve.report/api)

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