



# CVE-2013-1670

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

## Summary

|                        |                                                                                                                                                                                                                                                                                                                                                         |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2013-1670                                                                                                                                                                                                                                                                                                                                           |
| <b>State</b>           | PUBLIC                                                                                                                                                                                                                                                                                                                                                  |
| <b>Assigner</b>        | security@mozilla.org                                                                                                                                                                                                                                                                                                                                    |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                                                                                                                                                                                                                                            |
| <b>Published</b>       | 2013-05-16 11:45:00 UTC                                                                                                                                                                                                                                                                                                                                 |
| <b>Updated</b>         | 2017-09-19 01:36:00 UTC                                                                                                                                                                                                                                                                                                                                 |
| <b>Description</b>     | The Chrome Object Wrapper (COW) implementation in Mozilla Firefox before 21.0, Firefox ESR 17.x before 17.0.6, Thunderbird before 17.0.6, and SeaMonkey before 2.28.1.0 allows remote attackers to execute arbitrary code or cause a denial of service (memory consumption) via a crafted HTML document, as demonstrated by a proof of concept exploit. |

## Risk And Classification

**Problem Types:** CWE-264 | CWE-79

## NVD Known Affected Configurations (CPE 2.3)

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

| References                                                                       |  |  |  |            |                                       |      |
|----------------------------------------------------------------------------------|--|--|--|------------|---------------------------------------|------|
| Reference                                                                        |  |  |  | Source     | Link                                  | Tags |
| Debian -- Security Information -- DSA-2699-1 iceweasel                           |  |  |  | DEBIAN     | <a href="#">www.debian.org</a>        |      |
| Mozilla Firefox and Thunderbird CVE-2013-1670 Cross Site Scripting Vulnerability |  |  |  | BID        | <a href="#">www.securityfocus.com</a> |      |
| Firefox toString console.time Privileged Javascript Injection                    |  |  |  | EXPLOIT-DB | <a href="#">www.exploit-db.com</a>    |      |
| [security-announce] openSUSE-SU-2013:0834-1: important: MozillaThunderbird       |  |  |  | SUSE       | <a href="#">lists.opensuse.org</a>    |      |
| Red Hat Customer Portal                                                          |  |  |  | REDHAT     | <a href="#">rhn.redhat.com</a>        |      |

|                                                                        |                        |                                |  |
|------------------------------------------------------------------------|------------------------|--------------------------------|--|
| <a href="#">Debian -- Security Information -- DSA-2699-1 iceweasel</a> | <a href="#">DEBIAN</a> | <a href="#">www.debian.org</a> |  |
|------------------------------------------------------------------------|------------------------|--------------------------------|--|

|                                                                          |          |                                                                 |                 |
|--------------------------------------------------------------------------|----------|-----------------------------------------------------------------|-----------------|
| [security-announce] openSUSE-SU-2013:0825-1: important: MozillaFirefox:  | SUSE     | <a href="https://lists.opensuse.org">lists.opensuse.org</a>     |                 |
| 93427                                                                    | OSVDB    | <a href="https://www.osvdb.org">www.osvdb.org</a>               |                 |
| [security-announce] openSUSE-SU-2013:0946-1: important: MozillaFirefox:  | SUSE     | <a href="https://lists.opensuse.org">lists.opensuse.org</a>     |                 |
| Red Hat Customer Portal                                                  | REDHAT   | <a href="https://rhn.redhat.com">rhn.redhat.com</a>             |                 |
| Repository / Oval Repository                                             | OVAL     | <a href="https://oval.cisecurity.org">oval.cisecurity.org</a>   |                 |
| MFSA 2013-42: Privileged access for content level constructor            | CONFIRM  | <a href="https://www.mozilla.org">www.mozilla.org</a>           | Vendor Adviso   |
| USN-1822-1: Firefox vulnerabilities   Ubuntu                             | UBUNTU   | <a href="https://www.ubuntu.com">www.ubuntu.com</a>             |                 |
| Support / Security / Advisories / / MDVSA-2013:165   Mandriva            | MANDRIVA | <a href="https://www.mandriva.com">www.mandriva.com</a>         |                 |
| [security-announce] openSUSE-SU-2013:0831-1: important: xulrunner to 17. | SUSE     | <a href="https://lists.opensuse.org">lists.opensuse.org</a>     |                 |
| [security-announce] openSUSE-SU-2013:0929-1: important: xulrunner to 17. | SUSE     | <a href="https://lists.opensuse.org">lists.opensuse.org</a>     |                 |
| USN-1823-1: Thunderbird vulnerabilities   Ubuntu                         | UBUNTU   | <a href="https://www.ubuntu.com">www.ubuntu.com</a>             |                 |
| Access Denied                                                            | CONFIRM  | <a href="https://bugzilla.mozilla.org">bugzilla.mozilla.org</a> |                 |
| CVE Program record                                                       | CVE.ORG  | <a href="https://www.cve.org">www.cve.org</a>                   | canonical       |
| NVD vulnerability detail                                                 | NVD      | <a href="https://nvd.nist.gov">nvd.nist.gov</a>                 | canonical, anal |

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

**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)