



# CVE-2013-0757

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

## Summary

|                        |                                                                                                                                                                                                                                                                                                    |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2013-0757                                                                                                                                                                                                                                                                                      |
| <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 13:08:00 UTC                                                                                                                                                                                                                                                                            |
| <b>Description</b>     | The Chrome Object Wrapper (COW) implementation in Mozilla Firefox before 18.0, Firefox ESR 17.x before 17.0.2, Thunderbird before 17.0.8, and SeaMonkey before 2.28.10.0 is vulnerable to a buffer overflow attack. An attacker can exploit this to execute arbitrary code with system privileges. |

## Risk And Classification

### Problem Types: CWE-20

## 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                                 |  |  |
| [security-announce] SUSE-SU-2013:0048-1: important: Security update for                         |  |  | SUSE    | <a href="#">lists.opensuse.org</a>   |  |  |
| USN-1681-1: Firefox vulnerabilities   Ubuntu                                                    |  |  | UBUNTU  | <a href="#">www.ubuntu.com</a>       |  |  |
| 813901 – (CVE-2013-0757) Chrome Object Wrapper can be bypassed using Object.prototype.__proto__ |  |  | CONFIRM | <a href="#">bugzilla.mozilla.org</a> |  |  |
| [security-announce] openSUSE-SU-2013:0131-1: important: Mozilla Januarys                        |  |  | SUSE    | <a href="#">lists.opensuse.org</a>   |  |  |
| USN-1681-4: Firefox regression   Ubuntu                                                         |  |  | UBUNTU  | <a href="#">www.ubuntu.com</a>       |  |  |
| Repository / Oval Repository                                                                    |  |  | OVAL    | <a href="#">oval.cisecurity.org</a>  |  |  |
| USN-1681-2: Thunderbird vulnerabilities   Ubuntu                                                |  |  | UBUNTU  | <a href="#">www.ubuntu.com</a>       |  |  |
| MFSA 2013-14: Chrome Object Wrapper (COW) bypass through changing prototype                     |  |  | CONFIRM | <a href="#">www.mozilla.org</a>      |  |  |
| [security-announce] openSUSE-SU-2013:0149-1: important: Mozilla Januarys                        |  |  | SUSE    | <a href="#">lists.opensuse.org</a>   |  |  |
| [security-announce] SUSE-SU-2013:0049-1: important: Security update for                         |  |  | SUSE    | <a href="#">lists.opensuse.org</a>   |  |  |
| CVE Program record                                                                              |  |  | CVE.ORG | <a href="#">www.cve.org</a>          |  |  |

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)