



# CVE-2009-2477

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

## Summary

|                        |                                                                                                                                |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2009-2477                                                                                                                  |
| <b>State</b>           | PUBLIC                                                                                                                         |
| <b>Assigner</b>        | cve@mitre.org                                                                                                                  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                   |
| <b>Published</b>       | 2009-07-15 15:30:00 UTC                                                                                                        |
| <b>Updated</b>         | 2017-09-19 01:29:00 UTC                                                                                                        |
| <b>Description</b>     | js/src/jstracer.cpp in the Just-in-time (JIT) JavaScript compiler (aka TraceMonkey) in Mozilla Firefox 3.5 before 3.5.1 allows |

## Risk And Classification

### Problem Types: CWE-94

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                  | Product                 | Version | Update | Edition | Language |
|-------------|-------------------------|-------------------------|---------|--------|---------|----------|
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox</a> | 3.5     | All    | All     | All      |
| Application | <a href="#">Mozilla</a> | <a href="#">Firefox</a> | 3.5     | All    | All     | All      |

## References

| Reference                                                                                                                                | Source    |
|------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| MFSA 2009-41: Corrupt JIT state after deep return from native function                                                                   | CONFIRMED |
| Exploit – Page 40936 – Exploits Database                                                                                                 | EXPLOIT   |
| Mozilla Firefox 3.5 (Font tags) Remote Buffer Overflow Exploit                                                                           | EXPLOIT   |
| US-CERT Vulnerability Note VU#443060                                                                                                     | CERT      |
| Firefox 3.5 new exploit - confirmed                                                                                                      | MISC      |
| #266148: Multiple Security Vulnerabilities in Firefox Versions Prior to 3.5.2 May Allow Execution of Arbitrary Code or Application Crash | SUN       |
| Mozilla Firefox Two Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com                                       | SEC       |
| Security Fix - Stopgap Fix for Critical Firefox 3.5 Security Hole                                                                        | MISC      |
| [SECURITY] Fedora 11 Update: gnome-python2-extras-2.25.3-5.fc11                                                                          | FED       |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH                                                                         | VUP       |
| Mozilla Firefox 3.5 (Font tags) Remote Heap Spray Exploit                                                                                | EXPLOIT   |
| First Zero Day Exploit for Firefox 3.5 - The H Security: News and Features                                                               | MISC      |

|                                                                                          |     |
|------------------------------------------------------------------------------------------|-----|
| Bug 503286 – browser crash when search suggestions show [@ js_Interpret ] [@ js_Execute] | CON |
| Critical JavaScript vulnerability in Firefox 3.5 at Mozilla Security Blog                | CON |
| Mozilla Firefox 3.5 'TraceMonkey' Component Remote Code Execution Vulnerability          | BID |
| CVE Program record                                                                       | CVE |
| NVD vulnerability detail                                                                 | NVD |
| <div> <div></div> <div></div> </div>                                                     |     |
| 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](#)