



# CVE-2016-2790

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

|                        |                                                                                                                                |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2016-2790                                                                                                                  |
| <b>State</b>           | PUBLIC                                                                                                                         |
| <b>Assigner</b>        | security@mozilla.org                                                                                                           |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                   |
| <b>Published</b>       | 2016-03-13 18:59:00 UTC                                                                                                        |
| <b>Updated</b>         | 2019-12-27 16:08:00 UTC                                                                                                        |
| <b>Description</b>     | The graphite2::TtfUtil::GetTableInfo function in Graphite 2 before 1.3.6, as used in Mozilla Firefox before 45.0 and Firefox E |

## Risk And Classification

### Problem Types: CWE-19

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor  | Product     | Version | Update | Edition | Language |
|-------------|---------|-------------|---------|--------|---------|----------|
| Application | Mozilla | Firefox     | All     | All    | All     | All      |
| Application | Mozilla | Firefox Esr | 38.0    | All    | All     | All      |
| Application | Mozilla | Firefox Esr | 38.0.1  | All    | All     | All      |
| Application | Mozilla | Firefox Esr | 38.0.5  | All    | All     | All      |
| Application | Mozilla | Firefox Esr | 38.1.0  | All    | All     | All      |
| Application | Mozilla | Firefox Esr | 38.1.1  | All    | All     | All      |
| Application | Mozilla | Firefox Esr | 38.2.0  | All    | All     | All      |
| Application | Mozilla | Firefox Esr | 38.2.1  | All    | All     | All      |
| Application | Mozilla | Firefox Esr | 38.3.0  | All    | All     | All      |
| Application | Mozilla | Firefox Esr | 38.4.0  | All    | All     | All      |
| Application | Mozilla | Firefox Esr | 38.5.0  | All    | All     | All      |
| Application | Mozilla | Firefox Esr | 38.5.1  | All    | All     | All      |
| Application | Mozilla | Firefox Esr | 38.6.0  | All    | All     | All      |
| Application | Mozilla | Firefox Esr | 38.6.1  | All    | All     | All      |
| Application | Mozilla | Firefox Esr | 38.0    | All    | All     | All      |
| Application | Mozilla | Firefox Esr | 38.0.1  | All    | All     | All      |
| Application | Mozilla | Firefox Esr | 38.0.5  | All    | All     | All      |

|                  |          |                  |        |     |     |     |
|------------------|----------|------------------|--------|-----|-----|-----|
| Application      | Mozilla  | Firefox Esr      | 38.1.0 | All | All | All |
| Application      | Mozilla  | Firefox Esr      | 38.1.1 | All | All | All |
| Application      | Mozilla  | Firefox Esr      | 38.2.0 | All | All | All |
| Application      | Mozilla  | Firefox Esr      | 38.2.1 | All | All | All |
| Application      | Mozilla  | Firefox Esr      | 38.3.0 | All | All | All |
| Application      | Mozilla  | Firefox Esr      | 38.4.0 | All | All | All |
| Application      | Mozilla  | Firefox Esr      | 38.5.0 | All | All | All |
| Application      | Mozilla  | Firefox Esr      | 38.5.1 | All | All | All |
| Application      | Mozilla  | Firefox Esr      | 38.6.0 | All | All | All |
| Application      | Mozilla  | Firefox Esr      | 38.6.1 | All | All | All |
| Operating System | Opensuse | Leap             | 42.1   | All | All | All |
| Operating System | Opensuse | Leap             | 42.1   | All | All | All |
| Operating System | Opensuse | Opensuse         | 13.1   | All | All | All |
| Operating System | Opensuse | Opensuse         | 13.2   | All | All | All |
| Operating System | Opensuse | Opensuse         | 13.1   | All | All | All |
| Operating System | Opensuse | Opensuse         | 13.2   | All | All | All |
| Operating System | Oracle   | Linux            | 5.0    | All | All | All |
| Operating System | Oracle   | Linux            | 6      | All | All | All |
| Operating System | Oracle   | Linux            | 7      | All | All | All |
| Operating System | Oracle   | Linux            | 5.0    | All | All | All |
| Operating System | Oracle   | Linux            | 6      | All | All | All |
| Operating System | Oracle   | Linux            | 7      | All | All | All |
| Application      | Sil      | Graphite2        | All    | All | All | All |
| Operating System | Suse     | Linux Enterprise | 12.0   | All | All | All |
| Operating System | Suse     | Linux Enterprise | 12.0   | All | All | All |

## References

### Reference

USN-2917-3: Firefox regressions | Ubuntu

[security-announce] SUSE-SU-2016:0909-1: important: Security update for

Debian -- Security Information -- DSA-3520-1 icedove

Graphite2 library Multiple Security Vulnerabilities

USN-2934-1: Thunderbird vulnerabilities | Ubuntu

USN-2917-1: Firefox vulnerabilities | Ubuntu

Debian -- Security Information -- DSA-3510-1 iceweasel

USN-2927-1: Firefox vulnerabilities | Ubuntu

USN-2927-1: graphite2 vulnerabilities | Ubuntu

Mozilla Products: Multiple vulnerabilities (GLSA 201605-06) — Gentoo security

[security-announce] openSUSE-SU-2016:0733-1: important: Security update

[security-announce] SUSE-SU-2016:0820-1: important: Security update for

Mozilla Firefox Multiple Flaws Let Remote Users Execute Arbitrary Code, Spoof the Address Bar, Overwrite Files, and Deny Service - Security

[security-announce] openSUSE-SU-2016:0894-1: important: Security update

Debian -- Security Information -- DSA-3515-1 graphite2

Graphite: Multiple vulnerabilities (GLSA 201701-63) — Gentoo Security

Access Denied

Font vulnerabilities in the Graphite 2 library — Mozilla

[security-announce] openSUSE-SU-2016:0731-1: important: Security update

[security-announce] SUSE-SU-2016:0777-1: important: Security update for

Oracle Linux Bulletin - January 2016

[security-announce] openSUSE-SU-2016:1769-1: important: Security update

[security-announce] openSUSE-SU-2016:0876-1: important: Security update

USN-2917-2: Firefox regressions | Ubuntu

[security-announce] openSUSE-SU-2016:1778-1: important: Security update

[security-announce] openSUSE-SU-2016:1767-1: important: Security update

[security-announce] SUSE-SU-2016:0727-1: important: Security update for

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[710417](#) Gentoo Linux Graphite Multiple Vulnerabilities (GLSA 201701-63)

© [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](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)