



# CVE-2016-1521

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

## Summary

<b>CVE</b>	CVE-2016-1521
<b>State</b>	PUBLIC
<b>Assigner</b>	cert@cert.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2016-02-13 02:59:00 UTC
<b>Updated</b>	2017-07-01 01:29:00 UTC
<b>Description</b>	The directrun function in directmachine.cpp in Libgraphite in Graphite 2 1.2.4, as used in Mozilla Firefox before 43.0 and Fir

## Risk And Classification

### Problem Types: CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	7.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	7.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	22	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	23	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	22	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	23	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>	38.0.1	All	All	All
Application	<a href="#">Mozilla</a>	<a href="#">Firefox Esr</a>	38.0.5	All	All	All
Application	<a href="#">Mozilla</a>	<a href="#">Firefox Esr</a>	38.1.0	All	All	All
Application	<a href="#">Mozilla</a>	<a href="#">Firefox Esr</a>	38.1.1	All	All	All
Application	<a href="#">Mozilla</a>	<a href="#">Firefox Esr</a>	38.2.0	All	All	All
Application	<a href="#">Mozilla</a>	<a href="#">Firefox Esr</a>	38.2.1	All	All	All
Application	<a href="#">Mozilla</a>	<a href="#">Firefox Esr</a>	38.3.0	All	All	All
Application	<a href="#">Mozilla</a>	<a href="#">Firefox Esr</a>	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	38.5.2	All	All	All
Application	Mozilla	Firefox Esr	38.6.0	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	38.5.2	All	All	All
Application	Mozilla	Firefox Esr	38.6.0	All	All	All
Application	Mozilla	Thunderbird	All	All	All	All
Application	Sil	Graphite2	All	All	All	All

## References

Reference	Source	Link
[security-announce] SUSE-SU-2016:0779-1: important: Security update for	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>
[SECURITY] Fedora 22 Update: graphite2-1.3.6-1.fc22	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
Vulnerabilities in Graphite 2 — Mozilla	CONFIRM	<a href="http://www.mozilla.org">www.mozilla.org</a>
Red Hat Customer Portal	REDHAT	<a href="http://rhn.redhat.com">rhn.redhat.com</a>
[security-announce] openSUSE-SU-2016:0791-1: important: Security update	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>
[security-announce] openSUSE-SU-2016:0875-1: important: Security update	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>
Document Display   HPE Support Center	CONFIRM	<a href="http://h20566.www2.hp.com">h20566.www2.hp.com</a>
Oracle Linux Bulletin - April 2016	CONFIRM	<a href="http://www.oracle.com">www.oracle.com</a>
Graphite: Multiple vulnerabilities (GLSA 201701-63) — Gentoo Security	GENTOO	<a href="http://security.gentoo.org">security.gentoo.org</a>
Mozilla SeaMonkey: Multiple vulnerabilities (GLSA 201701-35) — Gentoo security	GENTOO	<a href="http://security.gentoo.org">security.gentoo.org</a>
[SECURITY] Fedora 23 Update: graphite2-1.3.5-1.fc23	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
Libgraphite Multiple Security Vulnerabilities	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>
Oracle Linux Bulletin - January 2016	CONFIRM	<a href="http://www.oracle.com">www.oracle.com</a>
Red Hat Customer Portal	REDHAT	<a href="http://rhn.redhat.com">rhn.redhat.com</a>

USN-2902-1: graphite2 vulnerabilities   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>
Cisco's Talos Intelligence Group Blog: Vulnerability Spotlight: Libgraphite Font Processing Vulnerabilities	MISC	<a href="http://blog.talosintel.com">blog.talosintel.com</a>
Debian -- Security Information -- DSA-3479-1 graphite2	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>
Red Hat Customer Portal	REDHAT	<a href="http://rhn.redhat.com">rhn.redhat.com</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

#### Legacy QID Mappings

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

[710447](#) Gentoo Linux Mozilla SeaMonkey Multiple Vulnerabilities (GLSA 201701-35)

© [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](http://status.cve.report)