



# CVE-2018-12405

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

## Summary

<b>CVE</b>	CVE-2018-12405
<b>State</b>	PUBLIC
<b>Assigner</b>	security@mozilla.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-02-28 18:29:00 UTC
<b>Updated</b>	2019-03-12 12:55:00 UTC
<b>Description</b>	Mozilla developers and community members reported memory safety bugs present in Firefox 63 and Firefox ESR 60.3. Sor

## 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="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.10	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>	9.0	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>	9.0	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="#">Thunderbird</a>	All	All	All	All

Application	Mozilla	Thunderbird	All	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All

## References

Reference	Source	Link	Tags
USN-3844-1: Firefox vulnerabilities   Ubuntu security notices	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	Third Party Advisory
Security vulnerabilities fixed in Firefox ESR 60.4 — Mozilla	CONFIRM	<a href="https://www.mozilla.org">www.mozilla.org</a>	Vendor Advisory
[SECURITY] [DLA 1605-1] firefox-esr security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	Third Party Advisory
Mozilla Firefox and Firefox ESR Multiple Security Vulnerabilities	BID	<a href="https://www.securityfocus.com">www.securityfocus.com</a>	Third Party Advisory, V
Debian -- Security Information -- DSA-4354-1 firefox-esr	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>	Third Party Advisory
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>	Third Party Advisory
Security vulnerabilities fixed in Firefox 64 — Mozilla	CONFIRM	<a href="https://www.mozilla.org">www.mozilla.org</a>	Vendor Advisory
Security vulnerabilities fixed in Thunderbird 60.4 — Mozilla	CONFIRM	<a href="https://www.mozilla.org">www.mozilla.org</a>	Vendor Advisory
Mozilla Firefox: Multiple vulnerabilities (GLSA 201903-04) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>	Third Party Advisory
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>	Third Party Advisory
USN-3868-1: Thunderbird vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	Third Party Advisory
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>	Third Party Advisory
Debian -- Security Information -- DSA-4362-1 thunderbird	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>	Third Party Advisory
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>	Third Party Advisory

Hed Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>	Third Party Advisory
Bug List	CONFIRM	<a href="https://bugzilla.mozilla.org">bugzilla.mozilla.org</a>	Broken Link, Issue Tra
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, analysis

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[710190](#) Gentoo Linux Mozilla Firefox Multiple Vulnerabilities (GLSA 201903-04)

© [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](https://status.cve.report)