



# CVE-2018-5168

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

## Summary

<b>CVE</b>	CVE-2018-5168
<b>State</b>	PUBLIC
<b>Assigner</b>	security@mozilla.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-06-11 21:29:00 UTC
<b>Updated</b>	2020-08-24 17:37:00 UTC
<b>Description</b>	Sites can bypass security checks on permissions to install lightweight themes by manipulating the "baseURI" property of the

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## 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>	17.10	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>	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>	17.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	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="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	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="#">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	Mozilla	Firefox ESR	All	All	All	All
Application	Mozilla	Thunderbird	All	All	All	All
Application	Mozilla	Thunderbird	All	All	All	All
Application	Mozilla	Thunderbird ESR	All	All	All	All
Application	Mozilla	Thunderbird ESR	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	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.5	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

Security vulnerabilities fixed in Firefox 60 — Mozilla

Debian -- Security Information -- DSA-4199-1 firefox-esr

Mozilla Firefox and Firefox ESR Multiple Security Vulnerabilities

USN-3645-1: Firefox vulnerabilities | Ubuntu security notices

Red Hat Customer Portal

[SECURITY] [DLA 1382-1] thunderbird security update

[SECURITY] [DLA 1376-1] firefox-esr security update

OpenSUSE Security Update: Firefox ESR 52.0.0 Mozilla

Security vulnerabilities fixed in Firefox ESR 52.8 — Mozilla

1449548 - (CVE-2018-5168) Lightweight themes can be installed automatically, without user's consent

Red Hat Customer Portal

Mozilla Firefox Multiple Bugs Let Remote Users Spoof Filenames, Bypass Security Restrictions, Obtain Potentially Sensitive Information, and

Debian -- Security Information -- DSA-4209-1 thunderbird

USN-3660-1: Thunderbird vulnerabilities | Ubuntu security notices

Security vulnerabilities fixed in Thunderbird 52.8 — Mozilla

Red Hat Customer Portal

Red Hat Customer Portal

Mozilla Thunderbird: Multiple vulnerabilities (GLSA 201811-13) — Gentoo security

Mozilla Firefox: Multiple vulnerabilities (GLSA 201810-01) — Gentoo security

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[690642](#) Free Berkeley Software Distribution (FreeBSD) Security Update for mozilla (5aefc41e-d304-4ec8-8c82-824f84f08244)

[710279](#) Gentoo Linux Mozilla Firefox Multiple Vulnerabilities (GLSA 201810-01)

[710285](#) Gentoo Linux Mozilla Thunderbird Multiple Vulnerabilities (GLSA 201811-13)

© [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](#)