

[RHSA-2019:0219-01] Critical: firefox security update

Article URL

www.securityhome.eu/mailings/mailling.php?mid=15004

Author

SecurityHome.eu

Published: 30 January 2019

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA256

=====
Red Hat Security Advisory

Synopsis: Critical: firefox security update
Advisory ID: RHSA-2019:0219-01
Product: Red Hat Enterprise Linux
Advisory URL: <https://access.redhat.com/errata/RHSA-2019:0219>
Issue date: 2019-01-30
CVE Names: CVE-2018-18500 CVE-2018-18501 CVE-2018-18505
=====

1. Summary:

An update for firefox is now available for Red Hat Enterprise Linux 7.

Red Hat Product Security has rated this update as having a security impact of Critical. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) in the References section.

2. Relevant releases/architectures:

Red Hat Enterprise Linux Client (v. 7) - x86_64
Red Hat Enterprise Linux Client Optional (v. 7) - x86_64
Red Hat Enterprise Linux Server (v. 7) - ppc64, ppc64le, s390x, x86_64
Red Hat Enterprise Linux Server Optional (v. 7) - x86_64
Red Hat Enterprise Linux Workstation (v. 7) - x86_64
Red Hat Enterprise Linux Workstation Optional (v. 7) - x86_64
Red Hat Enterprise Linux for ARM and IBM Power LE (POWER9) Server (v. 7) - aarch64, ppc64le, s390x

3. Description:

Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability.

This update upgrades Firefox to version 60.5.0 ESR.

Security Fix(es):

- * Mozilla: Use-after-free parsing HTML5 stream (CVE-2018-18500)
- * Mozilla: Memory safety bugs fixed in Firefox 65 and Firefox ESR 60.5 (CVE-2018-18501)
- * Mozilla: Privilege escalation through IPC channel messages (CVE-2018-18505)

For more details about the security issue(s), including the impact, a CVSS score, and other related information, refer to the CVE page(s) listed in the References section.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Yaniv Frank (SophosLabs), Alex Gaynor, Christoph Diehl, Steven Crane, Jason Kratzer, Gary Kwong, Christian Holler, and Jed Davis as the original reporters.

4. Solution:

For details on how to apply this update, which includes the changes described in this advisory, refer to:

<https://access.redhat.com/articles/11258>

After installing the update, Firefox must be restarted for the changes to take effect.

5. Bugs fixed (<https://bugzilla.redhat.com/>):

- 1670631 - CVE-2018-18500 Mozilla: Use-after-free parsing HTML5 stream
- 1670632 - CVE-2018-18501 Mozilla: Memory safety bugs fixed in Firefox 65 and Firefox ESR 60.5
- 1670633 - CVE-2018-18505 Mozilla: Privilege escalation through IPC channel messages

6. Package List:

Red Hat Enterprise Linux Client (v. 7):

Source:

firefox-60.5.0-2.el7.src.rpm

x86_64:

firefox-60.5.0-2.el7.x86_64.rpm

firefox-debuginfo-60.5.0-2.el7.x86_64.rpm

Red Hat Enterprise Linux Client Optional (v. 7):

x86_64:

firefox-60.5.0-2.el7.i686.rpm

firefox-debuginfo-60.5.0-2.el7.i686.rpm

Red Hat Enterprise Linux Server (v. 7):

Source:

firefox-60.5.0-2.el7.src.rpm

ppc64:

firefox-60.5.0-2.el7.ppc64.rpm

firefox-debuginfo-60.5.0-2.el7.ppc64.rpm

ppc64le:

firefox-60.5.0-2.el7.ppc64le.rpm

firefox-debuginfo-60.5.0-2.el7.ppc64le.rpm

s390x:

firefox-60.5.0-2.el7.s390x.rpm

firefox-debuginfo-60.5.0-2.el7.s390x.rpm

x86_64:

firefox-60.5.0-2.el7.x86_64.rpm

firefox-debuginfo-60.5.0-2.el7.x86_64.rpm

Red Hat Enterprise Linux for ARM and IBM Power LE (POWER9) Server (v. 7):

Source:

firefox-60.5.0-2.el7.src.rpm

aarch64:

firefox-60.5.0-2.el7.aarch64.rpm

firefox-debuginfo-60.5.0-2.el7.aarch64.rpm

ppc64le:

firefox-60.5.0-2.el7.ppc64le.rpm

firefox-debuginfo-60.5.0-2.el7.ppc64le.rpm

s390x:

firefox-60.5.0-2.el7.s390x.rpm

firefox-debuginfo-60.5.0-2.el7.s390x.rpm

Red Hat Enterprise Linux Server Optional (v. 7):

x86_64:
firefox-60.5.0-2.el7.i686.rpm
firefox-debuginfo-60.5.0-2.el7.i686.rpm

Red Hat Enterprise Linux Workstation (v. 7):

Source:
firefox-60.5.0-2.el7.src.rpm

x86_64:
firefox-60.5.0-2.el7.x86_64.rpm
firefox-debuginfo-60.5.0-2.el7.x86_64.rpm

Red Hat Enterprise Linux Workstation Optional (v. 7):

x86_64:
firefox-60.5.0-2.el7.i686.rpm
firefox-debuginfo-60.5.0-2.el7.i686.rpm

These packages are GPG signed by Red Hat for security. Our key and details on how to verify the signature are available from <https://access.redhat.com/security/team/key/>

7. References:

<https://access.redhat.com/security/cve/CVE-2018-18500>
<https://access.redhat.com/security/cve/CVE-2018-18501>
<https://access.redhat.com/security/cve/CVE-2018-18505>
<https://access.redhat.com/security/updates/classification/#critical>

8. Contact:

The Red Hat security contact is <secalert@redhat.com>. More contact details at <https://access.redhat.com/security/team/contact/>

Copyright 2019 Red Hat, Inc.