



RHSA-2019:1880 - Security Advisory

Issued: 2019-07-29 Updated: 2019-07-29

[Overview](#)[Updated Packages](#)

Synopsis

Low: curl security and bug fix update

Type/Severity

Security Advisory: Low

Red Hat Lightspeed patch analysis

Identify and remediate systems affected by this advisory.

[View affected systems](#) 

Topic

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

Red Hat Product Security has rated this update as having a security impact of Low. 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.

Description

The curl packages provide the libcurl library and the curl utility for downloading files from servers using various protocols, including HTTP, FTP, and LDAP.

Security Fix(es):

- curl: NTLM password overflow via integer overflow (CVE-2018-14618)

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

Bug Fix(es):

- baseurl with file:// hangs and then timeout in yum repo (BZ#1709474)
- curl crashes on http links with rate-limit (BZ#1711914)

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> 

Affected Products

- Red Hat Enterprise Linux Server 7 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 7.6 x86_64
- Red Hat Enterprise Linux Server - AUS 7.6 x86_64
- Red Hat Enterprise Linux Server - Extended Life Cycle Support 7 x86_64
- Red Hat Enterprise Linux Workstation 7 x86_64
- Red Hat Enterprise Linux Desktop 7 x86_64
- Red Hat Enterprise Linux for IBM z Systems 7 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 7.6 s390x
- Red Hat Enterprise Linux for Power, big endian 7 ppc64
- Red Hat Enterprise Linux for Power, big endian - Extended Update Support 7.6 ppc64
- Red Hat Enterprise Linux for Scientific Computing 7 x86_64
- Red Hat Enterprise Linux for Power, little endian 7 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 7.6 ppc64le
- Red Hat Enterprise Linux Server - TUS 7.6 x86_64
- Red Hat Enterprise Linux Server - Extended Life Cycle Support (for IBM z Systems) 7 s390x
- Red Hat Enterprise Linux for ARM 64 7 aarch64
- Red Hat Enterprise Linux for Power 9 7 ppc64le
- Red Hat Enterprise Linux EUS Compute Node 7.6 x86_64

- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 7.6 ppc64le
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 7.6 x86_64
- Red Hat Enterprise Linux for IBM System z (Structure A) 7 s390x
- Red Hat Enterprise Linux Server - Extended Life Cycle Support for IBM Power, big endian 7 ppc64
- Red Hat Enterprise Linux Server - Extended Life Cycle Support for IBM Power, little endian 7 ppc64le

Fixes

- [BZ - 1622707](#) - CVE-2018-14618 curl: NTLM password overflow via integer overflow
- [BZ - 1709474](#) - baseurl with file:// hangs and then timeout in yum repo [rhel-7.6.z]

CVEs

- [CVE-2018-14618](#)

References

- <https://access.redhat.com/security/updates/classification/#low>

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



Quick Links



Help



Site Info



Related Sites



 Partial system outage



[About Red Hat](#)

[Jobs](#)

[Events](#)

[Locations](#)

[Contact Red Hat](#)

[Red Hat Blog](#)

[Inclusion at Red Hat](#)

[Cool Stuff Store](#)

[Red Hat Summit](#)

© 2026 Red Hat

[Privacy statement](#)

[Terms of use](#)

[All policies and guidelines](#)

[Digital accessibility](#)

[Cookie preferences](#)