RHSA-2019:3701 - Security Advisory

Issued: 2019-11-05 Updated: 2019-11-05

Synopsis

Moderate: curl security and bug fix update

Type/Severity

Security Advisory: Moderate

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 8.

Red Hat Product Security has rated this update as having a security impact of Moderate. 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 type-2 heap out-of-bounds buffer read (CVE-2018-16890)
- wget: Information exposure in set_file_metadata function in xattr.c (CVE-2018-20483)
- curl: NTLMv2 type-3 header stack buffer overflow (CVE-2019-3822)
- curl: SMTP end-of-response out-of-bounds read (CVE-2019-3823)

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.

Additional Changes:

For detailed information on changes in this release, see the Red Hat Enterprise Linux 8.1 Release Notes linked from the References section.

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 for x86_64 8 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.8 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.8 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.6 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.6 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.4 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.4 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.2 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.1 x86_64
- Red Hat Enterprise Linux Server - AUS 8.6 x86_64
- Red Hat Enterprise Linux Server - AUS 8.4 x86_64
- Red Hat Enterprise Linux Server - AUS 8.2 x86_64
- Red Hat Enterprise Linux for IBM z Systems 8 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.8 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.6 s390x

- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.4 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.2 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.1 s390x
- Red Hat Enterprise Linux for Power, little endian 8 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.8 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.6 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.4 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.2 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.1 ppc64le
- Red Hat Enterprise Linux Server - TUS 8.8 x86_64
- Red Hat Enterprise Linux Server - TUS 8.6 x86_64
- Red Hat Enterprise Linux Server - TUS 8.4 x86_64
- Red Hat Enterprise Linux Server - TUS 8.2 x86_64
- Red Hat Enterprise Linux for ARM 64 8 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.8 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.6 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.4 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.2 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.1 aarch64
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.8 ppc64le
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.4 ppc64le
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.2 ppc64le
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.1 ppc64le
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.8 x86_64
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6 x86_64
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.4 x86_64
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.2 x86_64
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.1 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 8.10 x86_64
- Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 8.10 aarch64
- Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 8.10 ppc64le
- Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 8.10 s390x

Fixes

- BZ - 1662705 - CVE-2018-20483 wget: Information exposure in set_file_metadata function in xattr.c

- BZ - 1669156 - connection re-use does not work for SCP and SFTP
- BZ - 1670252 - CVE-2018-16890 curl: NTLM type-2 heap out-of-bounds buffer read
- BZ - 1670254 - CVE-2019-3822 curl: NTLMv2 type-3 header stack buffer overflow
- BZ - 1670256 - CVE-2019-3823 curl: SMTP end-of-response out-of-bounds read

CVEs

- CVE-2018-16890
- CVE-2018-20483
- CVE-2019-3822
- CVE-2019-3823

References

- https://access.redhat.com/security/updates/classification/#moderate
- https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/8.1_release_notes/

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

Loading