RHSA-2020:0594 - Security Advisory

Issued: 2020-02-25 Updated: 2020-02-25

Synopsis

Moderate: curl security 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 7.4 Advanced Update Support, Red Hat Enterprise Linux 7.4 Telco Extended Update Support, and Red Hat Enterprise Linux 7.4 Update Services for SAP Solutions.

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: HTTP authentication leak in redirects (CVE-2018-1000007)
- curl: FTP path trickery leads to NIL byte out of bounds write (CVE-2018-1000120)
- curl: RTSP RTP buffer over-read (CVE-2018-1000122)
- curl: Out-of-bounds heap read when missing RTSP headers allows information leak or denial of service (CVE-2018-1000301)
- curl: LDAP NULL pointer dereference (CVE-2018-1000121)

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.

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 - AUS 7.4 x86_64
- Red Hat Enterprise Linux Server - TUS 7.4 x86_64
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 7.4 ppc64le
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 7.4 x86_64

Fixes

- BZ - 1537125 - CVE-2018-1000007 curl: HTTP authentication leak in redirects
- BZ - 1552628 - CVE-2018-1000120 curl: FTP path trickery leads to NIL byte out of bounds write
- BZ - 1552631 - CVE-2018-1000121 curl: LDAP NULL pointer dereference
- BZ - 1553398 - CVE-2018-1000122 curl: RTSP RTP buffer over-read
- BZ - 1575536 - CVE-2018-1000301 curl: Out-of-bounds heap read when missing RTSP headers allows information leak or denial of service

CVEs

- CVE-2018-1000007
- CVE-2018-1000120
- CVE-2018-1000121
- CVE-2018-1000122
- CVE-2018-1000301

References

- https://access.redhat.com/security/updates/classification/#moderate

---

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