RHSA-2018:3157 - Security Advisory

Issued: 2018-10-30 Updated: 2018-10-30

Overview

Updated Packages

Synopsis

Moderate: curl and nss-pem 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 and nss-pem is now available for Red Hat Enterprise Linux 7.

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.

The nss-pem package provides the PEM file reader for Network Security Services (NSS) implemented as a PKCS#11 module.

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 of 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, and other related information, refer to the CVE page(s) listed in the References section.

Red Hat would like to thank the Curl project for reporting these issues. Upstream acknowledges Craig de Stigter as the original reporter of CVE-2018-1000007; Duy Phan Thanh as the original reporter of CVE-2018-1000120; Max Dymond as the original reporter of CVE-2018-1000122; the OSS-fuzz project as the original reporter of CVE-2018-1000301; and Dario Weisser as the original reporter of CVE-2018-1000121.

Additional Changes:

For detailed information on changes in this release, see the Red Hat Enterprise Linux 7.6 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 Server 7 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 Power, big endian 7 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 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 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 - 1510247 - make libcurl use the new PK11_CreateManagedGenericObject() function with nss-3.34 and newer
- BZ - 1537125 - CVE-2018-1000007 curl: HTTP authentication leak in redirects
- BZ - 1542256 - --tlsauthtype does not work (documentation only change)
- 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 of denial of service
- BZ - 1610998 - libcurl/curl >= 7.29.0-47 breaks yum update functionality on EC2 RHEL instances (401 unauthorized)

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
- https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/7.6_release_notes/index

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