



Cookie Preferences and Opt-Out Rights Your Choices About Cookies on this Site



Red Hat F

A cookie is a small amount of data that is sent to your browser from a web server and stored on your device. The cookie may be placed by Red Hat or by an authorized third party.

RHSA

3-10-30

Overview

When you use this site, Red Hat uses cookies and other technologies which are necessary to enable the basic features of the site to function (Required cookies). Subject to your preferences, Red Hat and its authorized partners may also use cookies to analyze your use of the website to evaluate and improve our performance, to improve our service to you and to personalize your experience (Functional cookies) as well as advertising cookies to show you ads that are more relevant to you (Advertising cookies). We honor the preferences you select.

Updated P

Synop

In addition to the services they provide to Red Hat, certain Red Hat authorized partners may also use this data for their own purposes or for targeted advertising. This activity may qualify as a "sale" or "targeted advertising" under certain data protection laws. You can make choices using the buttons below to allow or prevent such uses.

Moderat

Type/

Security

Accept default will keep your preferences set to accept all cookies (Required, Functional and Advertising), which enables us to provide you a personalized web experience and more relevant ads on third party websites. This means that you allow our partners to collect and use this data.

Red H

Identifi

View a

Required Cookies only will set your cookie preferences to "Required Cookies" only. This will prevent our partners from collecting and using this data but may also prevent us from providing you a personalized web experience and more relevant ads on third party websites. Cookie preferences will provide further information and allow you to customize your cookie settings. Setting your cookie preferences to "Required Cookies only" will opt you out of "sales" and "targeted advertising".

Topic

Clearing your browser cookies may delete your cookie preferences. If you re-

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/>.




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 and Opt-Out Rights](#)