

[Subscriptions](#) | [Downloads](#) | [Red Hat Capsule](#) | [Get Support](#)



Red Hat F

RHSA



2017-11-27

Overview

Updated P

Synop

Moderat

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.

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):

- A buffer overrun flaw was found in the IMAP handler of libcurl. By tricking an unsuspecting user into connecting to a malicious IMAP server, an attacker could exploit this flaw to potentially cause information disclosure or crash the application. (CVE-2017-1000257)

Red Hat would like to thank the Curl project for reporting this issue. Upstream acknowledges Brian Carpenter and the OSS-Fuzz project as the original reporters.

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 7.7 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 7.6 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 7.5 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 7.4 x86_64
- Red Hat Enterprise Linux Server - AUS 7.7 x86_64
- Red Hat Enterprise Linux Server - AUS 7.6 x86_64
- Red Hat Enterprise Linux Server - AUS 7.4 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 7.7 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 7.6 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 7.5 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 7.4 s390x
- Red Hat Enterprise Linux for Power, big endian 7 ppc64
- Red Hat Enterprise Linux for Power, big endian - Extended Update Support 7.7 ppc64
- Red Hat Enterprise Linux for Power, big endian - Extended Update Support 7.6 ppc64
- Red Hat Enterprise Linux for Power, big endian - Extended Update Support 7.5 ppc64

- Red Hat Enterprise Linux for Power, big endian - Extended Update Support 7.4 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 7.7 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 7.6 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 7.5 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 7.4 ppc64le
- Red Hat Enterprise Linux Server - TUS 7.7 x86_64
- Red Hat Enterprise Linux Server - TUS 7.6 x86_64
- Red Hat Enterprise Linux Server - TUS 7.4 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 7.7 x86_64
- Red Hat Enterprise Linux EUS Compute Node 7.6 x86_64
- Red Hat Enterprise Linux EUS Compute Node 7.5 x86_64
- Red Hat Enterprise Linux EUS Compute Node 7.4 x86_64
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 7.7 ppc64le
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 7.6 ppc64le
- 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 7.7 x86_64
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 7.6 x86_64
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 7.4 x86_64
- 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 - 1503705](#) - CVE-2017-1000257 curl: IMAP FETCH response out of bounds read



CVEs


- [CVE-2017-1000257](#)


References


- <https://access.redhat.com/security/updates/classification/#moderate>
- https://curl.haxx.se/docs/adv_20171023.html


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 Do Not Sell or Share My Personal Information](#)