RHSA-2018:3558 - Security Advisory

Issued: 2018-11-13 Updated: 2018-11-13

Synopsis

Moderate: httpd24 security, bug fix, and enhancement update

Type/Severity

Security Advisory: Moderate

Topic

An update for httpd24-httpd, httpd24-nghttp2, and httpd24-curl is now available for Red Hat Software Collections.

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 Apache HTTP Server is a powerful, efficient, and extensible web server. The httpd24 packages provide a recent stable release of version 2.4 of the Apache HTTP Server, along with the mod_auth_kerb module.

The following packages have been upgraded to a later upstream version: httpd24-httpd (2.4.34), httpd24-curl (7.61.1). (BZ#1590833, BZ#1648928)

Security Fix(es):

- httpd: Improper handling of headers in mod_session can allow a remote user to modify session data for CGI applications (CVE-2018-1283)
- httpd: Out of bounds read in mod_cache_socache can allow a remote attacker to cause DoS (CVE-2018-1303)
- httpd: mod_http2: Too much time allocated to workers, possibly leading to DoS (CVE-2018-1333)
- httpd: DoS for HTTP/2 connections by continuous SETTINGS frames (CVE-2018-11763)
- httpd: Out of bounds write in mod_authnz_ldap when using too small Accept-Language values (CVE-2017-15710)
- httpd: <FilesMatch> bypass with a trailing newline in the file name (CVE-2017-15715)
- httpd: Out of bounds access after failure in reading the HTTP request (CVE-2018-1301)
- httpd: Weak Digest auth nonce generation in mod_auth_digest (CVE-2018-1312)
- curl: Multiple security issues were fixed in httpd24-curl (CVE-2016-5419, CVE-2016-5420, CVE-2016-5421, CVE-2016-7141, CVE-2016-7167, CVE-2016-8615, CVE-2016-8616, CVE-2016-8617, CVE-2016-8618, CVE-2016-8619, CVE-2016-8620, CVE-2016-8621, CVE-2016-8622, CVE-2016-8623, CVE-2016-8624, CVE-2016-8625, CVE-2016-9586, CVE-2017-1000100, CVE-2017-1000101, CVE-2017-1000254, CVE-2017-1000257, CVE-2017-7407, CVE-2017-8816, CVE-2017-8817, CVE-2018-1000007, CVE-2018-1000120, CVE-2018-1000121, CVE-2018-1000122, CVE-2018-1000301, CVE-2018-14618)

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 CVE-2017-8816, CVE-2017-8817, CVE-2017-1000254, CVE-2017-1000257, CVE-2018-1000007, CVE-2018-1000120, CVE-2018-1000122, CVE-2018-1000301, CVE-2016-9586, CVE-2017-1000100, CVE-2017-1000101, CVE-2018-14618, and CVE-2018-1000121. Upstream acknowledges Alex Nichols as the original reporter of CVE-2017-8816; the OSS-Fuzz project as the original reporter of CVE-2017-8817 and CVE-2018-1000301; Max Dymond as the original reporter of CVE-2017-1000254 and CVE-2018-1000122; Brian Carpenter and the OSS-Fuzz project as the original reporters of CVE-2017-1000257; Craig de Stigter as the original reporter of CVE-2018-1000007; Duy Phan Thanh as the original reporter of CVE-2018-

1000120; Even Rouault as the original reporter of CVE-2017-1000100; Brian Carpenter as the original reporter of CVE-2017-1000101; Zhaoyang Wu as the original reporter of CVE-2018-14618; and Dario Weisser as the original reporter of CVE-2018-1000121.

Bug Fix(es):

- Previously, the Apache HTTP Server from the httpd24 Software Collection was unable to handle situations when static content was repeatedly requested in a browser by refreshing the page. As a consequence, HTTP/2 connections timed out and httpd became unresponsive. This bug has been fixed, and HTTP/2 connections now work as expected in the described scenario. (BZ#1518737)

Enhancement(s):

- This update adds the mod_md module to the httpd24 Software Collection. This module enables managing domains across virtual hosts and certificate provisioning using the Automatic Certificate Management Environment (ACME) protocol. The mod_md module is available only for Red Hat Enterprise Linux 7. (BZ#1640722)

Additional Changes:

For detailed information on changes in this release, see the Red Hat Software Collections 3.2 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

After installing the updated packages, the httpd daemon will be restarted automatically.

Affected Products

- Red Hat Software Collections (for RHEL Server) 1 for RHEL 7.7 x86_64
- Red Hat Software Collections (for RHEL Server for System Z) 1 for RHEL 7.7 s390x
- Red Hat Software Collections (for RHEL Server for IBM Power LE) 1 for RHEL 7.7 ppc64le
- Red Hat Software Collections (for RHEL Server) 1 for RHEL 7.6 x86_64
- Red Hat Software Collections (for RHEL Server for System Z) 1 for RHEL 7.6 s390x
- Red Hat Software Collections (for RHEL Server for IBM Power LE) 1 for RHEL 7.6 ppc64le
- Red Hat Software Collections (for RHEL Server) 1 for RHEL 7.5 x86_64
- Red Hat Software Collections (for RHEL Server for System Z) 1 for RHEL 7.5 s390x
- Red Hat Software Collections (for RHEL Server for IBM Power LE) 1 for RHEL 7.5 ppc64le
- Red Hat Software Collections (for RHEL Server) 1 for RHEL 7.4 x86_64

- Red Hat Software Collections (for RHEL Server for System Z) 1 for RHEL 7.4 s390x
- Red Hat Software Collections (for RHEL Server for IBM Power LE) 1 for RHEL 7.4 ppc64le
- Red Hat Software Collections (for RHEL Server) 1 for RHEL 7 x86_64
- Red Hat Software Collections (for RHEL Server for System Z) 1 for RHEL 7 s390x
- Red Hat Software Collections (for RHEL Server for IBM Power LE) 1 for RHEL 7 ppc64le
- Red Hat Software Collections (for RHEL Server for ARM) 1 aarch64
- Red Hat Software Collections (for RHEL Server) 1 for RHEL 6 x86_64
- Red Hat Software Collections (for RHEL Workstation) 1 for RHEL 7 x86_64
- Red Hat Software Collections (for RHEL Workstation) 1 for RHEL 6 x86_64

Fixes

- BZ - 1362183 - CVE-2016-5419 curl: TLS session resumption client cert bypass
- BZ - 1362190 - CVE-2016-5420 curl: Re-using connection with wrong client cert
- BZ - 1362199 - CVE-2016-5421 curl: Use of connection struct after free
- BZ - 1373229 - CVE-2016-7141 curl: Incorrect reuse of client certificates
- BZ - 1375906 - CVE-2016-7167 curl: escape and unescape integer overflows
- BZ - 1388370 - CVE-2016-8615 curl: Cookie injection for other servers
- BZ - 1388371 - CVE-2016-8616 curl: Case insensitive password comparison
- BZ - 1388377 - CVE-2016-8617 curl: Out-of-bounds write via unchecked multiplication
- BZ - 1388378 - CVE-2016-8618 curl: Double-free in curl_maprintf
- BZ - 1388379 - CVE-2016-8619 curl: Double-free in krb5 code
- BZ - 1388382 - CVE-2016-8620 curl: Glob parser write/read out of bounds
- BZ - 1388385 - CVE-2016-8621 curl: curl_getdate out-of-bounds read
- BZ - 1388386 - CVE-2016-8622 curl: URL unescape heap overflow via integer truncation
- BZ - 1388388 - CVE-2016-8623 curl: Use-after-free via shared cookies
- BZ - 1388390 - CVE-2016-8624 curl: Invalid URL parsing with '#'
- BZ - 1388392 - CVE-2016-8625 curl: IDNA 2003 makes curl use wrong host
- BZ - 1406712 - CVE-2016-9586 curl: printf floating point buffer overflow
- BZ - 1439190 - CVE-2017-7407 curl: --write-out out of bounds read
- BZ - 1478309 - CVE-2017-1000101 curl: URL globbing out of bounds read
- BZ - 1478310 - CVE-2017-1000100 curl: TFTP sends more than buffer size
- BZ - 1495541 - CVE-2017-1000254 curl: FTP PWD response parser out of bounds read
- BZ - 1503705 - CVE-2017-1000257 curl: IMAP FETCH response out of bounds read
- BZ - 1515757 - CVE-2017-8816 curl: NTLM buffer overflow via integer overflow
- BZ - 1515760 - CVE-2017-8817 curl: FTP wildcard out of bounds read
- BZ - 1518737 - HTTP/2 connections hang and timeout
- BZ - 1537125 - CVE-2018-1000007 curl: HTTP authentication leak in redirects
- BZ - 1540167 - provides without httpd24 pre/in-fix
- 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 - 1558450 - Not able to use SSLOpenSSLConfCmd with httpd24-httpd-2.4.27.
- BZ - 1560395 - CVE-2018-1283 httpd: Improper handling of headers in mod_session can allow a remote user to modify session data for CGI applications
- BZ - 1560399 - CVE-2018-1303 httpd: Out of bounds read in mod_cache_socache can allow a remote attacker to cause DoS
- BZ - 1560599 - CVE-2017-15710 httpd: Out of bounds write in mod_authnz_ldap when using too small Accept-Language values
- BZ - 1560614 - CVE-2017-15715 httpd: <FilesMatch> bypass with a trailing newline in the file name
- BZ - 1560634 - CVE-2018-1312 httpd: Weak Digest auth nonce generation in mod_auth_digest
- BZ - 1560643 - CVE-2018-1301 httpd: Out of bounds access after failure in reading the HTTP request
- BZ - 1575536 - CVE-2018-1000301 curl: Out-of-bounds heap read when missing RTSP headers allows information leak of denial of service
- BZ - 1605048 - CVE-2018-1333 httpd: mod_http2: Too much time allocated to workers, possibly leading to DoS
- BZ - 1622707 - CVE-2018-14618 curl: NTLM password overflow via integer overflow
- BZ - 1628389 - Make OCSP more configurable (like CRL)
- BZ - 1633260 - mod_session missing apr-util-openssl
- BZ - 1633399 - CVE-2018-11763 httpd: DoS for HTTP/2 connections by continuous SETTINGS frames
- BZ - 1634830 - FTBFS: httpd24-httpd
- BZ - 1640722 - mod_md is missing in httpd24-httpd
- BZ - 1646937 - Unable to start httpd
- BZ - 1648928 - Rebase curl to the latest version

CVEs

- CVE-2016-5419
- CVE-2016-5420
- CVE-2016-5421
- CVE-2016-7141
- CVE-2016-7167
- CVE-2016-8615
- CVE-2016-8616
- CVE-2016-8617
- CVE-2016-8618
- CVE-2016-8619
- CVE-2016-8620
- CVE-2016-8621

- CVE-2016-8622
- CVE-2016-8623
- CVE-2016-8624
- CVE-2016-8625
- CVE-2016-9586
- CVE-2017-7407
- CVE-2017-8816
- CVE-2017-8817
- CVE-2017-15710
- CVE-2017-15715
- CVE-2017-1000100
- CVE-2017-1000101
- CVE-2017-1000254
- CVE-2017-1000257
- CVE-2018-1283
- CVE-2018-1301
- CVE-2018-1303
- CVE-2018-1312
- CVE-2018-1333
- CVE-2018-11763
- CVE-2018-14618
- 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_software_collections/3/html/3.2_release_notes/chap-rhscl#sect-RHSCL-Changes-httpd

---

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

Red Hat

Quick Links

Help

Site Info

Related Sites

Loading

About Red Hat
Jobs
Events
Locations
Contact Red Hat
Red Hat Blog
Inclusion at Red Hat
Cool Stuff Store
Red Hat Summit