

[slackware-security] curl (SSA:2022-179-01)

Article URL

www.securityhome.eu/mailings/ mailing.php?mid=20962

Author

SecurityHome.eu

Published: 29 June 2022

[slackware-security] curl (SSA:2022-179-01)

New curl packages are available for Slackware 14.0, 14.1, 14.2, 15.0, and -current to fix security issues.

Here are the details from the Slackware 15.0 ChangeLog:

+-----+

patches/packages/curl-7.84.0-i586-1_slack15.0.txz: Upgraded.

This update fixes security issues:

Set-Cookie denial of service.

HTTP compression denial of service.

Unpreserved file permissions.

FTP-KRB bad message verification.

For more information, see:

<https://curl.se/docs/CVE-2022-32205.html>

<https://curl.se/docs/CVE-2022-32206.html>

<https://curl.se/docs/CVE-2022-32207.html>

<https://curl.se/docs/CVE-2022-32208.html>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-32205>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-32206>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-32207>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-32208>

(* Security fix *)

+-----+

Where to find the new packages:

+-----+

Thanks to the friendly folks at the OSU Open Source Lab (<http://osuosl.org>) for donating FTP and rsync hosting to the Slackware project! :-)

Also see the "Get Slack" section on <http://slackware.com> for additional mirror sites near you.

Updated package for Slackware 14.0:

ftp://ftp.slackware.com/pub/slackware/slackware-14.0/patches/packages/curl-7.84.0-i486-1_slack14.0.txz

Updated package for Slackware x86_64 14.0:

ftp://ftp.slackware.com/pub/slackware/slackware64-14.0/patches/packages/curl-7.84.0-x86_64-1_slack14.0.txz

Updated package for Slackware 14.1:

ftp://ftp.slackware.com/pub/slackware/slackware-14.1/patches/packages/curl-7.84.0-i486-1_slack14.1.txz

Updated package for Slackware x86_64 14.1:

ftp://ftp.slackware.com/pub/slackware/slackware64-14.1/patches/packages/curl-7.84.0-x86_64-1_slack14.1.txz

Updated package for Slackware 14.2:

ftp://ftp.slackware.com/pub/slackware/slackware-14.2/patches/packages/curl-7.84.0-i586-1_slack14.2.txz

Updated package for Slackware x86_64 14.2:

ftp://ftp.slackware.com/pub/slackware/slackware64-14.2/patches/packages/curl-7.84.0-x86_64-1_slack14.2.txz

Updated package for Slackware 15.0:

ftp://ftp.slackware.com/pub/slackware/slackware-15.0/patches/packages/curl-7.84.0-i586-1_slack15.0.txz

Updated package for Slackware x86_64 15.0:

ftp://ftp.slackware.com/pub/slackware/slackware64-15.0/patches/packages/curl-7.84.0-x86_64-1_slack15.0.txz

Updated package for Slackware -current:

<ftp://ftp.slackware.com/pub/slackware/slackware-current/slackware/n/curl-7.84.0-i586-1.txz>

Updated package for Slackware x86_64 -current:

ftp://ftp.slackware.com/pub/slackware/slackware64-current/slackware64/n/curl-7.84.0-x86_64-1.txz

MD5 signatures:

+-----+

Slackware 14.0 package:

d9e3d998503cffdbaeabc9249308154f curl-7.84.0-i486-1_slack14.0.txz

Slackware x86_64 14.0 package:

ca0bfae4c9e829109a44e044fdd3197d curl-7.84.0-x86_64-1_slack14.0.txz

Slackware 14.1 package:

415e395549d4f312ebe3f6d1ab2d5428 curl-7.84.0-i486-1_slack14.1.txz

Slackware x86_64 14.1 package:

f23c3a3e8d29496798521c4528aad486 curl-7.84.0-x86_64-1_slack14.1.txz

Slackware 14.2 package:

a575fe5b53d984466dd0996337cdbc18 curl-7.84.0-i586-1_slack14.2.txz

Slackware x86_64 14.2 package:

e878319393314356708eb2f13f036f7f curl-7.84.0-x86_64-1_slack14.2.txz

Slackware 15.0 package:

265458c2d664d37483848151ce3108c4 curl-7.84.0-i586-1_slack15.0.txz

Slackware x86_64 15.0 package:

5abab354c3d6cb386c0fd3a46e4941af curl-7.84.0-x86_64-1_slack15.0.txz

Slackware -current package:

f59680befc78cc6d8635324439443ade n/curl-7.84.0-i586-1.txz

Slackware x86_64 -current package:

174076dc227f904203d7f725d38bea7a n/curl-7.84.0-x86_64-1.txz

Installation instructions:

+-----+

Upgrade the package as root:

```
# upgradepkg curl-7.84.0-i586-1_slack15.0.txz
```

+-----+

Slackware Linux Security Team

<http://slackware.com/gpg-key>

security@slackware.com