



CVE-2023-31484

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2023-31484
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-04-29 00:15:00 UTC
Updated	2023-11-07 04:14:00 UTC
Description	CPAN.pm before 2.35 does not verify TLS certificates when downloading distributions over HTTPS.

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cpanpm Project	Cpanpm	All	All	All	All
Application	Perl	Perl	All	All	All	All

References

Reference

- oss-security - Perl's HTTP::Tiny has insecure TLS cert default, affecting CPAN.pm and other modules
- oss-security - Re: Perl's HTTP::Tiny has insecure TLS cert default, affecting CPAN.pm and other modules
- oss-security - Re: Perl's HTTP::Tiny has insecure TLS cert default, affecting CPAN.pm and other modules
- Changes - metacpan.org
- [SECURITY] Fedora 37 Update: perl-CPAN-2.36-1.fc37 - package-announce - Fedora Mailing-Lists
- Add verify_SSL=>1 to HTTP::Tiny in CPAN::HTTP::Client to verify https server identity by stigosp · Pull Request #175 · andk/cpanpm · GitHub
- [SECURITY] Fedora 37 Update: perl-CPAN-2.36-1.fc37 - package-announce - Fedora Mailing-Lists
- [SECURITY] Fedora 38 Update: perl-CPAN-2.36-1.fc38 - package-announce - Fedora Mailing-Lists
- Perl's HTTP::Tiny has insecure TLS default, affecting CPAN.pm and other modules – Hackeriet Blog
- oss-security - Re: Perl's HTTP::Tiny has insecure TLS cert default, affecting CPAN.pm and other modules
- oss-security - Re: Perl's HTTP::Tiny has insecure TLS cert default, affecting CPAN.pm and other modules
- [SECURITY] Fedora 38 Update: perl-CPAN-2.36-1.fc38 - package-announce - Fedora Mailing-Lists
- CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

161126 Oracle Enterprise Linux Security Update for perl-cpan (ELSA-2023-6539)
199391 Ubuntu Security Notification for Perl Vulnerability (USN-6112-2)
199482 Ubuntu Security Notification for Perl Vulnerability (USN-6112-1)
242292 Red Hat Update for perl-cpan (RHSA-2023:6539)
284306 Fedora Security Update for perl (FEDORA-2023-46924e402a)
284307 Fedora Security Update for perl (FEDORA-2023-1e5af38524)
330151 IBM AIX Vulnerability in perl (perl_advisory7)
355086 Amazon Linux Security Advisory for perl : ALAS2-2023-2034
355279 Amazon Linux Security Advisory for perl : ALAS2023-2023-178
355344 Amazon Linux Security Advisory for perl : ALAS-2023-1751
355401 Amazon Linux Security Advisory for perl-CPAN : ALAS2023-2023-182
673218 EulerOS Security Update for perl (EulerOS-SA-2023-2390)
673253 EulerOS Security Update for perl (EulerOS-SA-2023-2364)
673418 EulerOS Security Update for perl (EulerOS-SA-2023-2661)
673436 EulerOS Security Update for perl-cpan (EulerOS-SA-2023-3143)
673493 EulerOS Security Update for perl (EulerOS-SA-2023-2703)
673652 EulerOS Security Update for perl (EulerOS-SA-2023-3142)
673931 EulerOS Security Update for perl (EulerOS-SA-2023-2904)
674030 EulerOS Security Update for perl (EulerOS-SA-2023-2885)
755881 SUSE Enterprise Linux Security Update for perl (SUSE-SU-2023:2882-1)
908066 Common Base Linux Mariner (CBL-Mariner) Security Update for perl (37126)
941351 AlmaLinux Security Update for perl-CPAN (ALSA-2023:6539)

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)