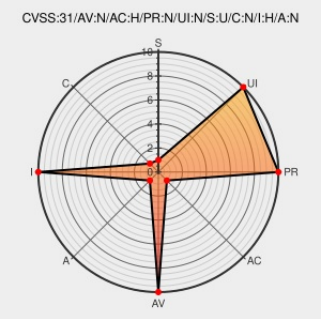
CVE-2014-3230

Published on: 01/28/2020 12:00:00 AM UTC

Last Modified on: 02/13/2023 12:08:09 AM UTC

CVE-2014-3230

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of from Lwp contain the following vulnerability:

The libwww-perl LWP::Protocol::https module 6.04 through 6.06 for Perl, when using IO::Socket::SSL as the SSL socket class, allows attackers to disable server certificate validation via the (1) HTTPS_CA_DIR or (2) HTTPS_CA_FILE environment variable.

CVE-2014-3230 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **libwww-perl** - **LWP::Protocol::https** version **= 6.04 through 6.06**

CVSS3 Score: 5.9 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	HIGH	NONE

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
oss-security - Re: Debian Bug#746579: libwww-perl: HTTPS_CA_DIR or HTTPS_CA_FILE disables peer certificate verification for IO::Socket::SSL	Mailing List Third Party Advisory www.openwall.com	MISC www.openwall.com/lists/oss-security/2014/05/06/8

	text/html	
oss-security - Re: Debian Bug#746579: libwww-perl: HTTPS_CA_DIR or HTTPS_CA_FILE disables peer certificate verification for IO::Socket::SSL	Mailing List Patch Third Party Advisory www.openwall.com text/html	MISC www.openwall.com/lists/oss-security/2014/05/04/1
#746579 - liblwp-protocol-https-perl: CVE-2014-3230: HTTPS_CA_DIR or HTTPS_CA_FILE disables peer certificate verification for IO::Socket::SSL - Debian Bug report logs	Exploit Mailing List Patch Third Party Advisory bugs.debian.org text/html	MISC bugs.debian.org/cgi-bin/bugreport.cgi?bug=746579
oss-security - Debian Bug#746579: libwww-perl: HTTPS_CA_DIR or HTTPS_CA_FILE disables peer certificate verification for IO::Socket::SSL	Mailing List Third Party Advisory www.openwall.com text/html	MISC www.openwall.com/lists/oss-security/2014/05/02/8
Unicorn! · GitHub	Broken Link github.com text/html Inactive Link Not Archived	MISC github.com/libwww-perl/lwp-protocol-https/pull/14

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Lwp		protocol		https_project	lwp
Application	Lwp		protocol\	\	https_project	lwp\

cpe:2.3:a:lwp::protocol::https_project:lwp::protocol::https:

cpe:2.3:a:lwp\:\:protocol\:\:https_project:lwp\:\:protocol\:\:https:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report