



# CVE-2020-14392

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

## Summary

<b>CVE</b>	CVE-2020-14392
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-09-16 13:15:00 UTC
<b>Updated</b>	2023-11-07 03:17:00 UTC
<b>Description</b>	An untrusted pointer dereference flaw was found in Perl-DBI < 1.643. A local attacker who is able to manipulate calls to dbc

## Risk And Classification

### Problem Types: CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	31	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.1	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.2	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.2	All	All	All
Application	<a href="#">Perl</a>	<a href="#">Database Interface</a>	All	All	All	All
Application	<a href="#">Perl</a>	<a href="#">Database Interface</a>	All	All	All	All

## References

Reference	Source	Link
[SECURITY] [DLA 2386-1] libdbi-perl security update	MLIST	<a href="#">list</a>
DBI::Changes - List of significant changes to the DBI - metacpan.org	MISC	<a href="#">me</a>
1877402 – (CVE-2020-14392) CVE-2020-14392 perl-dbi: Memory corruption in XS functions when Perl stack is reallocated	MISC	<a href="#">bu</a>
[security-announce] openSUSE-SU-2020:1502-1: important: Security update	SUSE	<a href="#">list</a>
[SECURITY] Fedora 31 Update: perl-DBI-1.643-3.fc31 - package-announce - Fedora Mailing-Lists		<a href="#">list</a>
[SECURITY] Fedora 31 Update: perl-DBI-1.643-3.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">list</a>
[security-announce] openSUSE-SU-2020:1483-1: important: Security update	SUSE	<a href="#">list</a>
USN-4503-1: Perl DBI module vulnerability   Ubuntu security notices   Ubuntu	UBUNTU	<a href="#">usi</a>
CVE Program record	CVE.ORG	<a href="#">ww</a>
NVD vulnerability detail	NVD	<a href="#">nv</a>

No vendor comments have been submitted for this CVE.

#### Legacy QID Mappings

- [500519](#) Alpine Linux Security Update for perl-dbi
- [501989](#) Alpine Linux Security Update for perl-dbi
- [504279](#) Alpine Linux Security Update for perl-dbi
- [670466](#) EulerOS Security Update for perl-DBI (EulerOS-SA-2021-2226)
- [671136](#) EulerOS Security Update for perl-DBI (EulerOS-SA-2021-2605)
- [750633](#) OpenSUSE Security Update for perl-DBI (openSUSE-SU-2020:1502-1)

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#).

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