



Crypt::DSA versions before 1.20 for Perl generate seeds using rand

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

Summary

CVE	CVE-2026-8700
State	PUBLISHED
Assigner	CPANSec
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-15 22:16:57 UTC
Updated	2026-05-16 01:16:17 UTC
Description	Crypt::DSA versions before 1.20 for Perl generate seeds using rand. Seeds were generated using Perl's built-in rand function.

Risk And Classification

Problem Types: CWE-331 | CWE-331 CWE-331 Insufficient Entropy

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	TIMLEGGE	CryptDSA	affected 1.20 custom	Not specified

References

Reference	Source	Link
www.openwall.com/lists/oss-security/2026/05/15/26	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com
metacpan.org/release/TIMLEGGE/Crypt-DSA-1.20/diff/TIMLEGGE/Crypt-DSA-1.19	9b29abf9-4ab0-4765-b253-1875cd9b441e	metacpan.org
metacpan.org/release/TIMLEGGE/Crypt-DSA-1.20/changes	9b29abf9-4ab0-4765-b253-1875cd9b441e	metacpan.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
CNA	2026-05-15T00:00:00.000Z	CPANSec identified issue
CNA	2026-05-15T00:00:00.000Z	Author was notified

CNA

2026-05-15T00:00:00.000Z

Version 1.20 released.

Solutions

CNA: Upgrade to version 1.20 or later.

There are currently no legacy QID mappings associated with this CVE.

© [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](#).

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

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