Net::Dropbear versions before 0.14 for Perl contains a vulnerable version of libtomcrypt

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2025-15638
State	PUBLISHED
Assigner	CPANSec
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-21 16:16:19 UTC
Updated	2026-04-22 17:35:37 UTC
Description	Net::Dropbear versions before 0.14 for Perl contains a vulnerable version of libtomcrypt. Net::Dropbear versions before 0.1

Risk And Classification

Primary CVSS: v3.1 10 CRITICAL from ADP

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Problem Types: NVD-CWE-noinfo | CWE-1395 CWE-1395 Dependency on Vulnerable Third-Party Component

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	10	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	10	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

High

ntegrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Atrodo	Net	\	dropbear	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	ATRODO	NetDropbear	affected 0.14 custom	Not specified

References

Reference	Source	Link
www.cve.org/CVERecord	9b29abf9-4ab0-4765-b253-1875cd9b441e	www.cve.o
metacpan.org/release/ATRODO/Net-Dropbear-0.14/source/dropbear/libtomcrypt/...	9b29abf9-4ab0-4765-b253-1875cd9b441e	metacpan.(
www.cve.org/CVERecord	9b29abf9-4ab0-4765-b253-1875cd9b441e	www.cve.o
CVE Program record	CVE.ORG	www.cve.o
NVD vulnerability detail	NVD	nvd.nist.go

No vendor comments have been submitted for this CVE.

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