Vulnerability in Cryptobox allows an authenticated user to trigger an account lockout

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

Summary

CVE	CVE-2026-5794
State	PUBLISHED
Assigner	THA-PSIRT
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-28 19:37:47 UTC
Updated	2026-04-28 20:10:23 UTC
Description	A vulnerability affecting the detailed versions of Cryptobox allows a legitimate user to prevent another to login by triggering

Risk And Classification

Primary CVSS: v4.0 4.9 MEDIUM from psirt@thalesgroup.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:U/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-694 | CWE-694 CWE-694 Use of multiple resources with duplicate identifier

Version	Source	Type	Score	Severity	Vector
4.0	psirt@thalesgroup.com	Secondary	4.9	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E
4.0	CNA	CVSS	4.9	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

None

ntegrity

None

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:U/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Ercom	Cryptobox	affected 4.40.175 semver	Not specified
CNA	Ercom	Cryptobox	affected 4.37.237 4.38.0 semver	Not specified

References

Reference	Source	Link	Tags
info.cryptobox.com/doc/v4.40/4.40.en	psirt@thalesgroup.com	info.cryptobox.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Solutions

CNA: Upgrade to version 4.40.177 or above.

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

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