



# Admin Passwords Cached by Browsers in Truesec LAPSWebUI

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

## Summary

<b>CVE</b>	CVE-2025-15554
<b>State</b>	PUBLISHED
<b>Assigner</b>	NCSC-FI
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-16 14:17:56 UTC
<b>Updated</b>	2026-04-07 00:50:55 UTC
<b>Description</b>	Browser caching of LAPS passwords in Truesec's LAPSWebUI before version 2.4 allows an attacker with access to a work

## Risk And Classification

**Primary CVSS:** v4.0 6 MEDIUM from db4dfee8-a97e-4877-bfae-eba6d14a2166

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

**EPSS:** 0.000150000 probability, percentile 0.027870000 (date 2026-04-07)

**Problem Types:** CWE-525 | CWE-525 CWE-525 Use of web browser cache containing sensitive information

Version	Source	Type	Score	Severity	Vector
4.0	db4dfee8-a97e-4877-bfae-eba6d14a2166	Secondary	6	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:P/VC:H/VI:N/VA:N/SC:H/SI:H/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
4.0	CNA	CVSS	6	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:P/VC:H/VI:N/VA:N/SC:H/SI:H/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
3.1	nvd@nist.gov	Primary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

## CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

Low

User Interaction

Passive

Confidentiality

High

Integrity

None

Availability

None

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

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

### CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Truesec	Lapswebui	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
--------	--------	---------	---------	-----------

Source	Vendor	Product	Version	Reference
CNA	Truesec	LAPSWebUI	affected 2.4 maven	Not specified
CNA	Truesec	LAPSWebUI	unaffected 2.4 maven	Not specified

## References

Reference	Source	Link
labs.reversesec.com/advisories/2026/03/admin-passwords-cached-by-browsers-in-true...	db4dfee8-a97e-4877-bfae-eba6d14a2166	labs.rev
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist

## Vendor Comments And Credit

### Discovery Credit

**CNA:** Laban Sköllermark at Reversesec Sweden AB (en)

## Additional Advisory Data

### Workarounds

**CNA:** Make sure the web server hosting LAPSWebUI sets the following HTTP response header: Cache-Control: no-store

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](#)