



DLL Hijacking in EfficientLab Controlio Leads to Local Privilege Escalation

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

Summary

CVE	CVE-2025-10549
State	PUBLISHED
Assigner	SEC-VLab
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-23 07:16:39 UTC
Updated	2026-04-23 07:16:39 UTC
Description	EfficientLab Controlio before v1.3.95 contains a DLL hijacking vulnerability caused by weak folder permissions in the install...

Risk And Classification

Problem Types: CWE-427 | CWE-427 CWE-427 Uncontrolled Search Path Element

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	EfficientLab LLC	Controlio	affected <1.3.95	Not specified

References

Reference	Source	Link
r.sec-consult.com/controlio	551230f0-3615-47bd-b7cc-93e92e730bbf	r.sec-consult.com/controlio
kb.controlio.net/hc/en-us/articles/45777908471185-Client-Update-April-15-2026-...	551230f0-3615-47bd-b7cc-93e92e730bbf	kb.controlio.net/hc/en-us/articles/45777908471185-Client-Update-April-15-2026-...
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Tobias Niemann, SEC Consult Vulnerability Lab (en)

CNA: Daniel Hirschberger, SEC Consult Vulnerability Lab (en)

CNA: Thorger Jansen, SEC Consult Vulnerability Lab (en)

CNA: Marius Renner, SEC Consult Vulnerability Lab (en)

Additional Advisory Data

Solutions

CNA: The vendor provides a patch v1.3.95 which should be installed immediately.

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](#)