Improper Limitation of a Pathname to a Restricted Directory Vulnerability on Multiple Products

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

Summary

CVE	CVE-2026-6865
State	PUBLISHED
Assigner	schneider
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-12 14:17:10 UTC
Updated	2026-05-12 14:19:41 UTC
Description	CWE-22: Improper Limitation of a Pathname to a Restricted Directory (“Path Traversal”) vulnerability that could cause unau

Risk And Classification

Primary CVSS: v4.0 7.1 HIGH from cybersecurity@se.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N/E:X/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-22 | CWE-22 CWE-22 Improper Limitation of a Pathname to a Restricted Directory (“Path Traversal”)

Version	Source	Type	Score	Severity	Vector
4.0	cybersecurity@se.com	Secondary	7.1	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N/E:
4.0	CNA	CVSS	7.1	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

High

ntegrity

Low

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N/E:X/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
CNA	Schneider Electric	EasyLogic T150 Formerly Saitel DR Remote Terminal Unit Controller	affected Versions 11.06.31 and prior
CNA	Schneider Electric	Saitel DP Remote Terminal Unit Controller	affected Versions 11.06.36 and prior

References

Reference	Source	Link	Tags
download.schneider-electric.com/files	cybersecurity@se.com	download.schneider-electric.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.

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