Simopro Technology | WinMatrix - Missing Authentication

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

Summary

CVE	CVE-2026-6348
State	PUBLISHED
Assigner	twcert
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-16 03:16:30 UTC
Updated	2026-04-17 15:38:09 UTC
Description	WinMatrix agent developed by Simopro Technology has a Missing Authentication vulnerability, allowing authenticated local

Risk And Classification

Primary CVSS: v4.0 9.3 CRITICAL from twcert@cert.org.tw

CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/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/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000080000 probability, percentile 0.006580000 (date 2026-04-20)

Problem Types: CWE-306 | CWE-306 CWE-306 Missing authentication for critical function

Version	Source	Type	Score	Severity	Vector
4.0	twcert@cert.org.tw	Secondary	9.3	CRITICAL	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:X/(
4.0	CNA	CVSS	9.3	CRITICAL	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H
3.1	twcert@cert.org.tw	Primary	8.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
3.1	CNA	CVSS	8.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/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/MSC: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

Changed

Confidentiality

High

Integrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Simopro Technology	WinMatrix	affected 3.5.13 3.5.26.15 custom	Not specified

References

Reference	Source	Link	Tags
www.twcert.org.tw/en/cp-139-10840-ba9b9-2.html	twcert@cert.org.tw	www.twcert.org.tw	
www.twcert.org.tw/tw/cp-132-10839-2d9a7-1.html	twcert@cert.org.tw	www.twcert.org.tw	
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: Update agent to version 3.5.27.5 or later.

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