

Vector Tool Installer (Windows)

Important Security Information

Document Management		
Author	Vector Informatik GmbH	
Status	Released	
Version Date	1.0	01.09.2026
Change History		

Vector Tool Installer (Windows)

Security Vulnerabilities

Following security vulnerabilities within the Vector Tool Installer (Windows) has been discovered lately.

CVE-ID pending DLL Search Order Hijacking in Vector Tool Installer (Windows)

Note: The CVE-ID for this vulnerability has been requested from MITRE and had not yet been assigned at the time of this publication.

Applicability

Uncontrolled search path elements in the Vector Tool Installer (Windows) versions allow local privilege escalation via DLL search-order hijacking. The installer loads DLLs (e.g., msi.dll) from its own directory after UAC elevation, enabling arbitrary code execution **if a malicious DLL is planted alongside the installer**.

This issue is fixed in the Vector Tool Installer version 2605a released on 20.08.2026.

We identified the following affected Vector Products:

Product Name / Version	Patched Installer available
CANape	Planned for 23SP5, 24SP3HF2, 24SP4 (Sep. 2026)
CANdelaStudio	Planned for 25 SP1 P1 Planned for 24 P12
CANoe DE & SE (Linux installer is not affected)	Done for 19 SP6
Windows Installation via Chocolatey is not affected	Done for 20 SP2.1
DYNA4	Done for DYNA4 R10 SP1 (v10.1.1) Done for DYNA4 R10 (v10.0.6)
CANoe Model Option Vehicle and Driver	Alongside DYNA4 R10 SP1 (line above)
CANoe Model Option Electric Motor	Alongside DYNA4 R10 SP1 (line above)
LDF Explorer	Planned for 1.7.41
FIBEX Explorer	Planned for 3.5.5
AUTOSAR-viewer	Planned for 1.8.7
AUTOSAR-preprocessor	Planned for 12.1.9
vVIRTUALtarget	Planned for 10 SP3
CANoe Test Package VAG	Planned for 5.2 SP3
vFlash	Planned for 11 SP5 (Sept. 2026) Planned for 12 SP2 (Sept. 2026) Planned for 13 (Dec. 2026)
vTESTstudio	Done for 11 SP2
SOVD2UDS Adapter	Planned for 1 SP4 (Sep. 2026)
ODXStudio	Planned for 15 (Dec. 2026)
CANoe Emulation Package EV	Planned for 2.0 (Sep. 2026)
CANoe Test Package EV	Planned for 9.0
CANoe Test Package EVSE	Planned for 7.0 (Oct. 2026)
vSignalalyzer	Planned for 23SP5, 24SP3HF2, 24SP4 (Sep. 2026)
vMeasure	Planned for 9SP5, 10SP4 (Sep. 2026)
D-PDU API	Planned 1 SP21 (Sept 2026)
PassThru	Planned 1 SP17 (Sept 2026)
DaVinci External Components	Planned for 3.8.0 (Sep 2026)
Vector Tool Platform	Planned for 7.5 (Oct 2026)

Vector License Client	Planned for 9.4 (Oct 2026)
-----------------------	----------------------------

For other versions see **Recommended Actions** as workaround.

Risk Analysis

CVSS 4.0 Severity and Vector Strings:

CVSS-B 7 HIGH

Vector: CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

CVSS 3.x Severity and Vector Strings:

Base Score: 7.8 HIGH

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

Common Weakness Enumeration (CWE)

CWE-427 - Uncontrolled Search Path Element:

The product uses a fixed or controlled search path to find resources, but one or more locations in that path can be under the control of unintended actors.

If you successfully installed our products with one of the affected Installers in the past, you are not affected by this CVE. It only occurs during installation.

Recommended Actions

Make sure that no other files (e.g. DLLs) are in the same directory when running an installer until fixed versions of these are available.

Do not trust installers from unreliable sources (e.g. installers in zips with other files). Do not trust DLLs from unreliable sources.

Credits

Thank you to Koki Takase for reporting this issue.

We will inform you by updating this advisory.