TLP:WHITE

VDE-2025-063: Phoenix Contact: Device and Update Management Windows Installer Privilege Escalation

Publisher: Phoenix Contact GmbH & Co. KG	Document category: csaf_security_advisory
Initial release date: Tue Aug 12 12:00:00 CEST 2025	Engine: 2.5.32
Current release date: Tue Aug 12 12:00:00 CEST 2025	Build Date: Tue Aug 05 15:20:42 CEST 2025
Current version: 1	Status: FINAL
CVSSv3.1 Base Score: 7.8	Severity: High
Original language: en	Language: en-GB
Also referred to: VDE-2025-063, PCSA-2025/00010	

Summary

A privilege escalation vulnerability exists in Phoenix Contact Device and Update Management prior to version 2025.3.1 due to misconfigured permissions on nssm.exe in the DAUM-WINDOWS-SERVICE. This misconfiguration allows a low-privileged local user to execute arbitrary code with administrative privileges.

General Recommendation

Phoenix Contact recommends operating network-capable devices in closed networks or protected with a suitable firewall. For detailed information on our recommendations for measures to protect network-capable devices, please refer to our application note.

Impact

The products installer allows privileges escalation to admin rights caused by the nssm.exe. Nssm.exe is an open-source tool designed to simplify the management of Windows services. The permissions on the nssm.exe were not secured properly, this could allow an attack to escalate privileges from a low privileged user to an administrator.

Remediation

Update to the latest 2025.3.1 DaUM Version.

Vulnerabilities

CVE-2025-41686

Vulnerability Description

A low-privileged local attacker can exploit improper permissions on nssm.exe to escalate their privileges and gain administrative access.

CWE: CWE-306: Missing Authentication for Critical Function

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
DaUM <2025.3.1 Order number: 1542953	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8

Fixed

Product
DaUM 2025.3.1 Order number: 1542953 (Download)

Acknowledgments

Phoenix Contact GmbH & Co. KG thanks the following parties for their efforts:

- CERT@VDE for coordination. (see: https://certvde.com)

Phoenix Contact GmbH & Co. KG

Namespace: https://phoenixcontact.com/psirt

psirt@phoenixcontact.com

References

- PCSA-2025/00010 (EXTERNAL): https://phoenixcontact.com/psirt
- Phoenix Contact advisory overview at CERT@VDE (EXTERNAL): https://certvde.com/de/advisories/vendor/phoenixcontact/
- Phoenix Contact application note (EXTERNAL): https://dam-mdc.phoenixcontact.com/asset/156443151564/0a870ae433c19148b80bd760f3a1c1f2/107913_en_03.pdf
- VDE-2025-063: Phoenix Contact: Device and Update Management Windows Installer Privilege Escalation - HTML (SELF): https://certvde.com/en/advisories/VDE-2025-063
- VDE-2025-063: Phoenix Contact: Device and Update Management Windows Installer Privilege Escalation - CSAF (SELF): https://phoenixcontact.csaf-tp.certvde.com/.well-known/csaf/white/2025/vde-2025-063.json

Revision history

Version	Date of the revision	Summary of the revision
1	Tue Aug 12 12:00:00 CEST 2025	Initial

Sharing rules

TLP:WHITE

For the TLP version see https://www.first.org/tlp/