



# Execution with Unnecessary Privileges

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

## Summary

<b>CVE</b>	CVE-2025-9966
<b>State</b>	PUBLISHED
<b>Assigner</b>	CyberDanube
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-09-23 12:15:29 UTC
<b>Updated</b>	2026-03-31 13:16:13 UTC
<b>Description</b>	Improper privilege management vulnerability in Novakon P series allows attackers to gain root privileges if one service is cc

## Risk And Classification

**Primary CVSS:** v4.0 7.3 HIGH from office@cyberdanube.com

**CVSS:**4.0/AV:P/AC:H/AT:P/PR:H/UI:A/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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**EPSS:** 0.000180000 probability, percentile 0.043760000 (date 2026-04-02)

**Problem Types:** CWE-269 | CWE-269 CWE-269 Improper Privilege Management

Version	Source	Type	Score	Severity	Vector
4.0	office@cyberdanube.com	Secondary	7.3	HIGH	CVSS:4.0/AV:P/AC:H/AT:P/PR:H/UI:A/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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
4.0	CNA	CVSS	7.3	HIGH	CVSS:4.0/AV:P/AC:H/AT:P/PR:H/UI:A/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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

## CVSS v4.0 Breakdown

Attack Vector

Physical

Attack Complexity

High

Attack Requirements

Present

Privileges Required

High

User Interaction

Active

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

CVSS:4.0/AV:P/AC:H/AT:P/PR:H/UI:A/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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Novakon	P Series P07 P10 P12 P15	affected P – V2001.A.c518o2 P-V2005 custom	Linux

### References

Reference	Source	Link
<a href="http://www.novakon.com.tw/common/frontend/download">www.novakon.com.tw/common/frontend/download</a>	office@cyberdanube.com	www
<a href="https://seclists.org/fulldisclosure/2025/Sep/70">seclists.org/fulldisclosure/2025/Sep/70</a>	af854a3a-2127-422b-91ae-364da2661108	sec
<a href="https://cyberdanube.com/security-research/multiple-vulnerabilities-in-novakon-hmi-series">cyberdanube.com/security-research/multiple-vulnerabilities-in-novakon-hmi-series</a>	office@cyberdanube.com	cyb
<a href="http://www.novakon.com.tw/en/news/detail/Security_Advisory__Firmware_Update_Available_f...">www.novakon.com.tw/en/news/detail/Security_Advisory__Firmware_Update_Available_f...</a>	office@cyberdanube.com	www
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd

### Vendor Comments And Credit

#### Discovery Credit

**CNA:** S. Dietz (CyberDanube) (en)

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](https://www.mitre.org/) and the authoritative source of CVE content is [MITRE's CVE web](https://www.mitre.org/cve/)

[site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)**