Execution with Unnecessary Privileges

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2025-9966
State	PUBLISHED
Assigner	CyberDanube
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-09-23 12:15:29 UTC
Updated	2026-03-31 13:16:13 UTC
Description	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/MSC:X/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
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

CVSS v4.0 Breakdown

Attack Vector

Physical

Attack Complexity

High

Attack Requirements

Present

Privileges Required

High

User Interaction

Active

Confidentiality

High

ntegrity

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/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	Platforms
CNA	Novakon	P Series P07 P10 P12 P15	affected P – V2001.A.c518o2 P-V2005 custom	Linux

References

Reference	Source	Lin
www.novakon.com.tw/common/frontend/download	office@cyberdanube.com	ww
seclists.org/fulldisclosure/2025/Sep/70	af854a3a-2127-422b-91ae-364da2661108	sec
cyberdanube.com/security-research/multiple-vulnerabilities-in-novakon-hmi-series	office@cyberdanube.com	cyb
www.novakon.com.tw/en/news/detail/Security_Advisory__Firmware_Update_Available_f...	office@cyberdanube.com	ww
CVE Program record	CVE.ORG	ww
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.

site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report