



Unauthenticated Buffer Overflow

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

Summary

CVE	CVE-2025-9962
State	PUBLISHED
Assigner	CyberDanube
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-09-23 11:15:39 UTC
Updated	2026-03-31 13:16:11 UTC
Description	A buffer overflow vulnerability in Novakon P series allows attackers to gain root permission without prior authentication. This

Risk And Classification

Primary CVSS: v4.0 10 CRITICAL from office@cyberdanube.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000810000 probability, percentile 0.239670000 (date 2026-04-02)

Problem Types: CWE-120 | CWE-120 CWE-120 Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Version	Source	Type	Score	Severity	Vector
4.0	office@cyberdanube.com	Secondary	10	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA
4.0	CNA	CVSS	10	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/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/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
www.novakon.com.tw/common/frontend/download	office@cyberdanube.com	www
seclists.org/fulldisclosure/2025/Sep/70	af854a3a-2127-422b-91ae-364da2661108	seclists
cyberdanube.com/security-research/multiple-vulnerabilities-in-novakon-hmi-series	office@cyberdanube.com	cyberdanube
www.novakon.com.tw/en/news/detail/Security_Advisory__Firmware_Update_Available_f...	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, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)