

1. Overview

NOVAKON has confirmed and addressed multiple security vulnerabilities (CVE-2025-9962 through CVE-2025-9966) affecting P Series HMI products.

The reported vulnerabilities have been fixed through an updated software release delivered via iFACE Designer 2.0.05 (Build 2026.02.09, commit 5ce397b9).

Customers are strongly recommended to update affected devices to the latest firmware version to ensure system security.

Status: Fixed

2. Affected Products

P07/P10/P12/P15

3. Remediation / Solution

The vulnerabilities described in this advisory are fixed in the following firmware release:

- Distribution package: iFACE Designer 2.0.05
- Build: 2026.02.09 (commit 5ce397b9)
- Contained firmware version: P-2.0.05 Build 2026.02.06 (commit d0f97fd9)

Customers should install the latest iFACE Designer release and apply the included firmware update to affected P Series HMI devices.

The corrective firmware may be installed using one of the following supported methods:

- Using iFACE Designer to install firmware via USB device or TCP/IP connection to the HMI.
- Transferring the firmware file included in the iFACE Designer installation directory to a USB device or SD card, and installing it directly on the HMI.

4. Temporary Mitigations and Recommended Security Practices

If the affected device cannot be updated immediately, the following temporary mitigations are recommended to minimize potential risks:

1. Use the HMI only in a protected environment to minimize network exposure and ensure that it is not accessible from the public Internet or any untrusted networks.
2. Restrict access to trusted internal networks only.
3. Verify software and firmware integrity prior to installation using the SHA-256 checksums provided by NOVAKON.

After applying the corrective update, the specific risks associated with CVE-2025-9962 through CVE-2025-9966 are mitigated. However, NOVAKON continues to recommend operating the HMI in a protected and trusted network environment and avoiding exposure to public Internet or untrusted networks as part of standard defense-in-depth security practices.

Use of legacy firmware versions should be considered only as an exception and does not eliminate the need to apply the latest security updates.

5. Patch Release and Verification

NOVAKON has released a corrective firmware update addressing CVE-2025-9962 through CVE-2025-9966 via the following software package:

- iFACE Designer version: 2.0.05
- Build: 2026.02.09 (commit 5ce397b9)

The corrective firmware included in this release is:

- Firmware version: P-V2005

Integrity verification information:

- SHA-256 checksum (iFACE Designer 2.0.05 installation package):
 - 9f6c5a502f07e193d3f9d69320a5bedd5a0aa517fd7479e5ab6d11fe24af401a
- SHA-256 checksum (firmware file P-V2005)
 - 3111b3bab3243a924c9fc7ba3eda9acd379f4cdeb7d058d496b6cce149c53003

Customers should verify the integrity of both the iFACE Designer installation package and the firmware file prior to installation, and follow official installation guidance during deployment.

6. Legacy Firmware Downgrade

Considerations

Due to long-term deployment of P Series HMI products in existing industrial environments, certain legacy systems may require continued operation with earlier firmware versions for compatibility or operational reasons.

To reduce unintended security exposure, firmware downgrade is **intentionally restricted to manual installation using removable media only** (USB device or SD card). Network-based downgrade mechanisms are not supported.

When attempting to install legacy firmware, the system will display the following warning message:

Warning: Installing legacy firmware may introduce known security risks and impact operation. Press OK to continue.

NOVAKON **does not recommend** downgrading to legacy firmware versions. Customers who choose to perform a downgrade should be aware that older firmware versions may contain known security vulnerabilities that have been addressed in newer releases.

Whenever possible, customers are strongly encouraged to operate devices using the **latest software and firmware versions** to maintain the highest level of security and reliability.

7. Incident Closure and Internal Feedback (CAPA)

Following remediation, the PSIRT will perform a structured post-incident review to identify root causes, implement corrective and preventive actions (CAPA), and strengthen internal secure development and vulnerability management practices.

The review outcomes are documented in the company's security improvement log and periodically evaluated by management as part of NOVAKON's

continuous-improvement activities.

8. Acknowledgements

NOVAKON would like to thank the following researcher for identifying and responsibly reporting these vulnerabilities and for supporting coordinated disclosure:

Sebastian Dietz (CyberDanube)

9. Contact Information

For assistance or inquiries regarding this advisory:

security@novakon.com.tw

10. Revision History

Version	Date	Description
1.0	2025-11-04	Initial publication of advisory.
2.0	2026-02-09	Fixed vulnerabilities via iFACE Designer 2.0.05 (Build 2026.02.09); added distribution details, supported installation paths, dual SHA-256 verification, mitigation applicability update, and legacy downgrade considerations