Out-of-bounds Read vulnerability in IPC platform NY-series

Release date: November 17, 2025
OMRON Corporation

■Overview

Out-of-bounds Read vulnerability (CWE-125) was found in the TPM 2.0 in the Industrial PC platform NY-series. Attackers may be able to read sensitive information or cause a denial of service by exploiting this vulnerability.

The products and versions affected by these vulnerabilities, mitigation and protection measures are shown below. Make sure to implement these recommended mitigations and protections to minimize the risk of exploitation of these vulnerabilities. Moreover, to ensure that customers use our products with confidence, the security enhanced countermeasure version of each product will be prepared. Please check countermeasure shown below in this document and implement appropriate countermeasure.

■Affected products

Affected products and versions are below.

Industrial PC platform NY-series

Model	TPM Version	Lot No. (Date of Manufacture)
NYB27-[][][][][]	5.63 or lower	Until 23X25 (October 23, 2025)
NYB35-[][][][][]		
NYB2C-[][][][][]		
NYB2A-[][][][][]		
NYB55-[][][][][]	7.85 or lower	
NYB65-[][][][][]		
NYB13-[][][][][]		
NYB37-[][][][][]		
NYB3A-[][][][][]		
NYB2E-[][][][][]		
NYP27-[][][][][]	5.63 or lower	
NYP35-[][][][][]		
NYP2C-[][][][][]		
NYP2A-[][][][][]		
NYP55-[][][][][]	7.85 or lower	
NYP65-[][][][][]		
NYP13-[][][][][]		
NYP37-[][][][][]		
NYP3A-[][][][][]		
NYE2A-[][][][][]	5.63 or lower	

Appendix below provides instructions on how to determine the version of the TPM in the NY Product.

Refer to “ID Information Label” section in the manuals below to check the product Lot no.

- NYB Industrial Box PC Hardware User’s Manual (W553)
- NYP Industrial Panel PC Hardware User’s Manual (W555)
- NYE Industrial Panel PC Hardware User's Manual (W634)

■Description

A vulnerability was found in the TPM 2.0 reference implementation code published by the Trusted Computing Group, Revisions 1.83, 1.59 and 1.38 which could potentially result in information disclosure or denial of service of the TPM.

This issue affects the Trusted Platform Module of the Industrial PC. Any data protected by the TPM, including data protected by BitLocker, is potentially vulnerable to this issue.

NYB/NYP/NYE Industrial PC users who do not take advantage of the TPM Security Features are not affected by this issue.

■CWE,CVE,CVSS Scores

Out-of-bounds Read (CWE-125)

CVE-2025-2884

CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:H Base Score 6.6

■Countermeasure

Update your TPM to fix this vulnerability. The versions to be applied are shown in the table below.

Industrial PC platform NY-series

Model	TPM Version	Lot No.	Release Date
NYB27-[][][][][]	5.66 or higher	24X25 or later	October 24, 2025
NYB35-[][][][][]			
NYB2C-[][][][][]			
NYB2A-[][][][][]			
NYB55-[][][][][]	7.86 or higher		
NYB65-[][][][][]			
NYB13-[][][][][]			
NYB37-[][][][][]			
NYB3A-[][][][][]			
NYB2E-[][][][][]			
NYP27-[][][][][]	5.66 or higher		
NYP35-[][][][][]			
NYP2C-[][][][][]			
NYP2A-[][][][][]			
NYP55-[][][][][]	7.86 or higher		
NYP65-[][][][][]			
NYP13-[][][][][]			
NYP37-[][][][][]			
NYP3A-[][][][][]			
NYE2A-[][][][][]	5.66 or higher		

Patch Image Release Date : November 4, 2025

Caution: If the TPM update fails, the IPC may fail to start.

Please proceed with the following steps only if you can accept this risk.

Instructions for updating the TPM

1. Go to OMRON download page [https://www.ia.omron.com/product/tool/ipc-platform/index.htm]
2. At the bottom of the page please read Software License Agreement and click "Agree the terms and move to download" for the latest version
3. Download the image corresponding to your IPC model from [Trusted Platform Module Firmware]
   Ensure SHA256 hash of downloaded image is the same as on download page
4. Using Rufus [https://rufus.ie/en/] create bootable USB flash drive from the downloaded image
5. Press the [DEL] key repeatedly, launch IPC into the BIOS
6. Select Advanced ~ Trusted Computing
7. Select Security Device Support: Disable
8. Save changes (F10). Restart
9. Connect the UEFI shell USB stick
10. Restart the IPC and boot into the USB stick
11. TPM update script will run automatically, wait until it finishes
12. Restart the IPC and launch it into the BIOS
13. Go to Advanced ~ Trusted Computing and set Security Device Support back to enable

■Mitigations and Protections

OMRON recommends that customers take the following mitigation measures to minimize the risk of exploitation of this vulnerability.

1. Anti-virus protection
   Protect any PC with access to the control system against malware and ensure installation and maintenance of up-to-date commercial grade anti-virus software protection.

2. Security measures to prevent unauthorized access
   - Minimize connection of control systems and equipment to open networks, so that untrusted devices will be unable to access them.
   - Implement firewalls (by shutting down unused communications ports, limiting communications hosts) and isolate them from the IT network.
   - Use a virtual private network (VPN) for remote access to control systems and equipment.
   - Use strong passwords and change them frequently.
   - Install physical controls so that only authorized personnel can access control systems and equipment.
   - Scan virus to ensure safety of any USB drives or similar devices before connecting them to systems and devices.
   - Enforce multifactor authentication to all devices with remote access to control systems and equipment whenever possible.

3. Data input and output protection
   Validation processing such as backup and range check to cope with unintentional modification of input/output data to control systems and devices.

4. Data recovery
   Periodical data backup and maintenance to prepare for data loss.

■Contact information

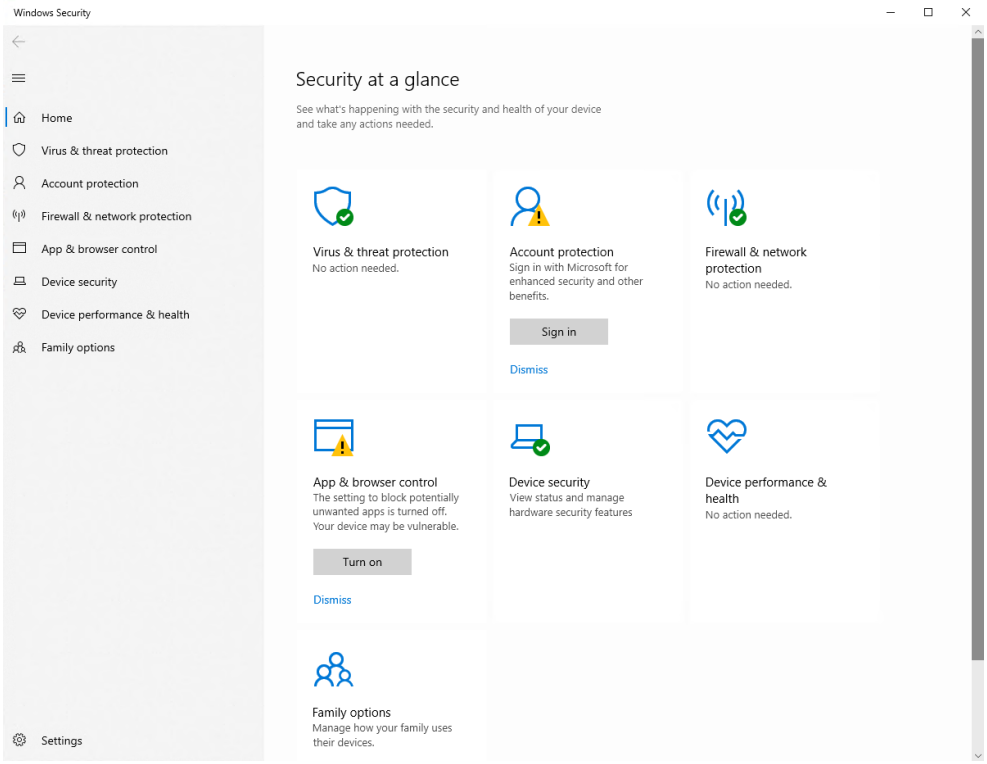
Please contact our sales office or distributors.
https://www.ia.omron.com/global_network/index.html

■Update history

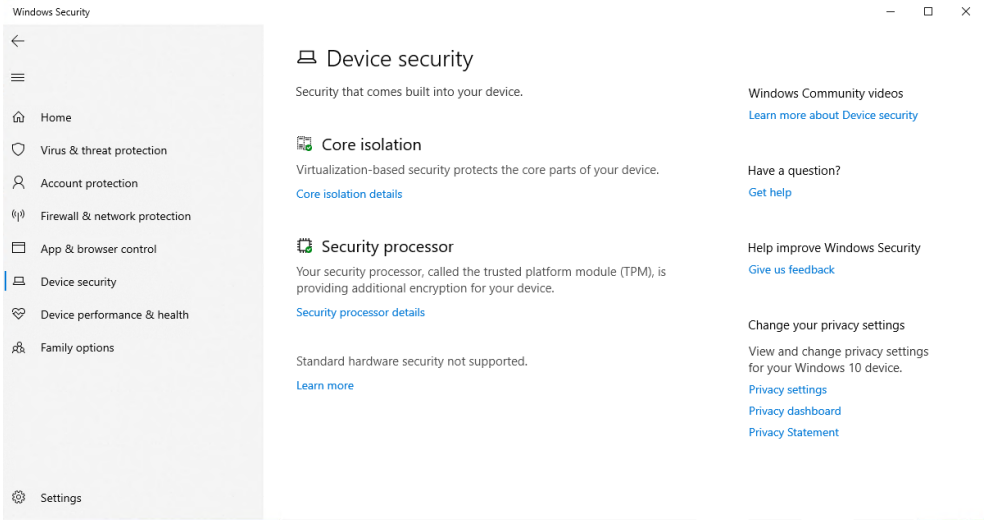
- November 17, 2025: New Release

Appendix – How to check TPM Version

1. In Windows, navigate to **Windows Security**
   The Windows Security information is shown:



2. Select **Device security**
   The Device security information is shown:



3. Select **Security processor details**

   The Security processor details are shown, including the manufacturer version of the TPM: