

IPC 平台 NY 系列存在越界读取漏洞

发布日期：2025 年 11 月 17 日

欧姆龙株式会社

■概要

欧姆龙一直致力于在工业自动化领域为客户提供安全、可靠、高质量的产品与解决方案，这是我们立足行业，持续助推客户业务增长，为客户创造价值的根基。

近期，我们发现工业 PC 平台 NY 系列的 TPM 2.0 存在越界读取（CWE-125）漏洞。攻击者可利用这些漏洞读取敏感信息，导致系统崩溃。

为了使您的安全得到有效保护，我们第一时间采取行动，排查受该漏洞影响的产品和版本，并推出相应对策、以及减轻措施/解决方法。您可以通过下述推荐的减轻措施/解决方法，实现将该漏洞的恶意利用风险降至最低。

此外，为了确保您安心使用本产品，我们还为受该漏洞影响的产品准备了安全增强的对策版本。您可在下文“对策方法”处查找对应的对策版本。

■对象产品

受此漏洞影响的产品型号及版本如下所示。

工业 PC 平台 NY 系列

型号	适用 TPM 版本	批号（生产日期）
NYB27-□□□□□	5.63 以下	23X25（2025 年 10 月 23 日）之前
NYB35-□□□□□		
NYB2C-□□□□□		
NYB2A-□□□□□		
NYB55-□□□□□	7.85 以下	
NYB65-□□□□□		
NYB13-□□□□□		
NYB37-□□□□□		
NYB3A-□□□□□		
NYB2E-□□□□□		
NYP27-□□□□□	5.63 以下	
NYP35-□□□□□		
NYP2C-□□□□□		
NYP2A-□□□□□		
NYP55-□□□□□	7.85 以下	
NYP65-□□□□□		
NYP13-□□□□□		
NYP37-□□□□□		
NYP3A-□□□□□		
NYE2A-□□□□□	5.63 以下	

确认 NY 系列 TPM 版本的方法，请参见“附件-TPM 版本的确认方法”。

确认批号的方法，请参见以下手册的“ID Information Label”。

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

■漏洞内容

可信计算组织 (Trusted Computing Group) 发布的 TPM 2.0 参考实现代码 (Rev 1.83、1.59、1.38) 中发现越界读取漏洞 (CWE-125), 该漏洞可能导致 TPM 中的信息泄露或拒绝服务攻击。

该漏洞会影响工业 PC 中的可信平台模块 (TPM)。包括受 BitLocker 保护的数据在内, 受 TPM 保护的
任何数据都可能受到影响。

因此, 使用 NYB/NYP/NYE 系列工业 PC 且不使用 TPM 安全功能的用户不会受到影响。

■CWE、CVE、CVSS 评分

越界读取(CWE-125)

CVE-2025-2884

CVSS: 3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:H 基础评分 6.6

■对策方法

将各产品的 TPM 更新至对策版本以应对漏洞。
各产品的对策版本与发布日期见下表。

工业 PC 平台 NY 系列

型号	适用 TPM 版本	批号	对策版本推出时间
NYB27-□□□□□	5.66 以上	24X25 之后	2025 年 10 月 24 日
NYB35-□□□□□			
NYB2C-□□□□□			
NYB2A-□□□□□			
NYB55-□□□□□	7.86 以上		
NYB65-□□□□□			
NYB13-□□□□□			
NYB37-□□□□□			
NYB3A-□□□□□			
NYB2E-□□□□□			
NYP27-□□□□□	5.66 以上		
NYP35-□□□□□			
NYP2C-□□□□□			
NYP2A-□□□□□			
NYP55-□□□□□	7.86 以上		
NYP65-□□□□□			
NYP13-□□□□□			
NYP37-□□□□□			
NYP3A-□□□□□			
NYE2A-□□□□□	5.66 以上		

补丁的发布日期：2025 年 11 月 4 日

注意：如果 TPM 更新失败，IPC 可能无法启动。

只有愿意承担风险时，才应执行以下步骤。

TPM 的更新步骤

1. 访问欧姆龙下载页面[<https://www.fa.omron.co.jp/member/product/tool/ipc-platform/index.htm>]
2. 请阅读页面底部的软件使用承诺合约书，然后点击“同意并下载”以获取最新版本。
3. 从[Trusted Platform Module 固件]下载与您的 IPC 型号对应的补丁。
确认下载补丁的 SHA256 哈希值是否与下载页面上列出的值匹配。
4. 使用 Rufus [<https://rufus.ie/ja/>] 从下载的补丁创建可启动的 USB 闪存。
5. 反复按下[DEL]键，通过 BIOS 启动 IPC。
6. 选择[Advanced]→[Trusted Computing]。
7. 选择[Security Device Support]，设定为[Disable]。
8. 保存变更后再启动。
9. 连接 UEFI shell 用 USB 存储器。
10. 再启动 IPC，从 USB 存储器启动。
11. TPM 更新脚本将自动运行，请等待其完成。
12. 再启动 IPC，通过 BIOS 启动。
13. 选择[Advanced]→[Trusted Computing]→[Security Device Support]，返回[Enable]。

■减轻措施/解决方法

为了实现将这些漏洞的恶意利用风险降至最低，我们十分建议您采取以下减轻措施。

1. 防病毒保护

在连接控制系统的电脑上安装最新版本的企业级杀毒软件，并定期维护。

2. 防止未经授权的访问

推荐采取以下措施。

- 最大限度地减少控制系统或设备的网络连接，禁止不受信任的设备访问
- 通过部署防火墙隔离 IT 网络（断开未使用的通信端口、限制通信主机）
- 需要远程访问控制系统或设备时，使用虚拟专用网络（VPN）
- 使用高强度密码并定期修改
- 引入物理控制，确保仅授权人员可访问控制系统和设备
- 在控制系统或设备中使用 USB 存储器等外部存储设备时，事先进行病毒扫描
- 在远程访问控制系统或设备时进行多重要素验证

3. 数据输入/输出保护

确认备份和范围检查等设置的合理性，以防对控制系统和设备的输入/输出数据的意外修改

4. 恢复丢失的数据

定期对设置数据进行备份和维护，以防数据丢失

■咨询方式

如您在采取减轻措施/解决方法时遇到问题，可以通过下列方式向我们的事务所或经销商咨询：

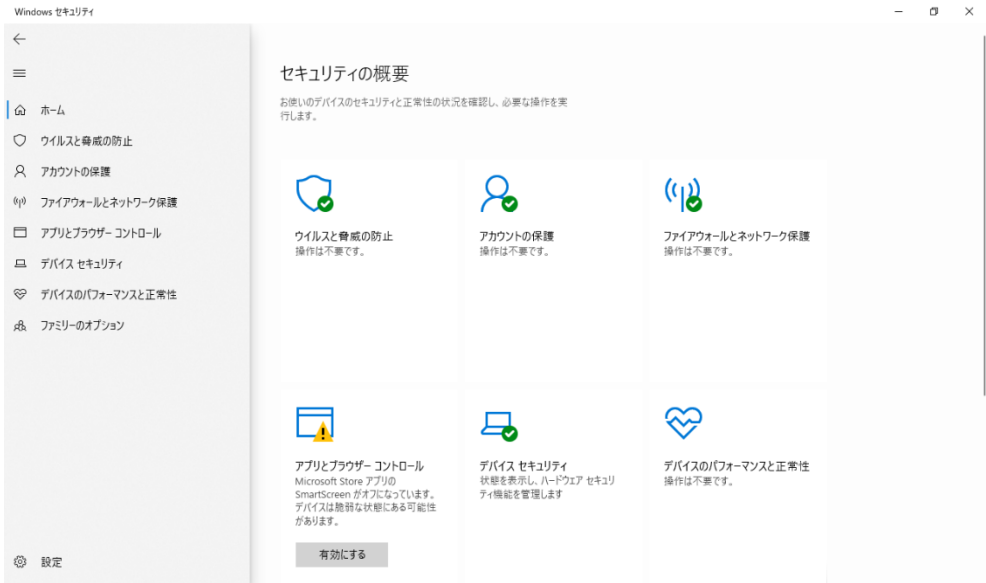
<https://www.fa.omron.com.cn/contactus>

■更新记录

2025 年 11 月 17 日：创建

附件-TPM 版本的确认方法

1. 在 Windows 中，转到[Windows 安全中心]。
显示 Windows 安全中心的信息。



2. 选择[设备安全性]。
显示设备安全性信息。



3. 选择[安全处理器详情]。
显示安全处理器详情，包括 TPM 制造商版本。

