BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2025-34
Fecha de publicación: 7/05/2025
Tema: Vulnerabilidad crítica en productos Honeywell
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

- Versiones de MB-Secure a partir de la V11.04 y anteriores a la V12.53
- Versiones de MB-Secure PRO a partir de la V01.06 y anteriores a la V03.09

Descripción

Se ha reportado una vulnerabilidad crítica en los paneles de control de alarma MB-Secure y MB-Secure PRO de Honeywell. La falla, identificada como CVE-2025-2605 con un score CVSSv3 de 9.9 (Crítico), permite a atacantes con acceso limitado ejecutar comandos no autorizados del sistema operativo con privilegios elevados, lo que supone un grave riesgo de vulnerabilidad del sistema.

Los componentes vulnerables exponen un punto de entrada donde se podrían inyectar y ejecutar comandos de sistema maliciosos sin las verificaciones de autorización adecuadas, lo que permite efectivamente la escalada de privilegios y la manipulación remota de los sistemas de alarma.

Solución

El equipo Honeywell recomienda una actualización urgente de sus paneles:

- Actualización a la versión V12.53 de MB-Secure
- Actualización a MB-Secure PRO versión V03.09

https://automation.honeywell.com/us/en/support/software-downloads
https://www.honeywellhome.com/us/en/support/

Si no puede realizar la actualización recomendamos que acuda al servicio de soporte del proveedor para recibir indicaciones de como hacerlo.

Información adicional:

- https://www.honeywell.com/content/dam/honeywellbt/en/documents/downloads/product-security/security-notification/hon-corp-os-command-injection-honeywell-mb-secure-2025-05-01-01.pdf
- https://nvd.nist.gov/vuln/detail/CVE-2025-2605

BEACON LAB

C S I R T

CYBOLT

Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com