Honeywell

SECURITY NOTICE

SN 2025-05-01-01: OS COMMAND INJECTION IN HONEYWELL MB-SECURE - (CVE-2025-2605)

Commented [JY1]: GREEN text indicates instructions and guidance that should be deleted for Final Submission

YELLOW highlights indicate information that should be changed or added that are specific to the particular Notice.

This article contains:

It applies to:
MB-Secure and MB-Secure PRO

Skills prerequisite:
Qualified personnel with administrative credentials.

Executive Summary

Honeywell is aware of a vulnerability in MB-Secure and MB-Secure PRO. This vulnerability could allow an attacker to execute operating system command leading to CAPEC-122: Privilege Abuse. This issue has been assigned CVE-2025-2605 and rated with a severity of Critical. Honeywell strongly recommends that users upgrade to the version identified below to resolve the vulnerability.

Vulnerability Synopsis

OS Command Injection in MB-Secure and MB-Secure PRO – (CVE-2025-2605)

MB-Secure and MB-Secure PRO alarm control panels were discovered to contain OS command injection in versions prior to V12.53 for MB-Secure and V03.09 for MB-Secure PRO. This can allow an attacker to execute malicious commands with elevated permissions.

CVSS Base Score: 9.9 (Critical)

CVSS Vector:
https://www.first.org/cvss/calculator/3-1#CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

CVE Number: CVE-2025-2605
https://nvd.nist.gov/vuln/detail/CVE-2025-2605

Honeywell

Affected Products

Product(s)/ Component(s)	CVE	Advisory/Update
MB-Secure versions from V11.04 and prior to V12.53	CVE-2025-2605	Upgrade to MB-Secure version V12.53
MB-Secure PRO versions from V01.06 and prior to V03.09	CVE-2025-2605	Upgrade to MB-Secure PRO version V03.09

Remediation

The vulnerability has been remediated in MB-Secure release V12.53 and MB-Secure PRO release V03.09. Honeywell strongly recommends that users upgrade to MB-Secure release V12.53 and MB-Secure PRO release V03.09, respectively.

Acknowledgments

Honeywell thanks Lukas Donaubauer, Senior Security Consultant at SEC Consult, for reporting this vulnerability.

References

- https://nvd.nist.gov/vuln/detail/CVE-2025-2605

Honeywell

Appendix: About CVSS

The Common Vulnerability Scoring System (CVSS) is an open standard for communicating the characteristics and severity of software vulnerabilities. The Base score represents the intrinsic qualities of a vulnerability. The Temporal score reflects the characteristics of a vulnerability that change over time. The Environmental score is an additional score that can be used by CVSS but is not supplied as it will differ for each customer.

The Base score has a value ranging from 0 to 10. The Temporal score has the same range and is a modification of the Base score due to current temporary factors.

The severity of the score can be summarized as follows:

Severity Rating	CVSS Score
None	0.0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score.

Detailed information about CVSS can be found at http://www.first.org/cvss.

DISCLAIMERS

- CUSTOMERS ARE RESPONSIBLE FOR ASSESSING THE IMPACT OF ANY ACTUAL OR POTENTIAL SECURITY VULNERABILITY. CUSTOMER'S FAILURE TO IMPLEMENT THE RECOMMENDED UPDATES OR ACTIONS, INCLUDING WITHOUT LIMITATION, RECOMMENDED PATCHES OR UPDATES TO ANY SOFTWARE OR DEVICE, SHALL BE AT CUSTOMER'S SOLE RISK AND EXPENSE. CUSTOMER SHALL TAKE ALL APPROPRIATE ACTIONS TO SECURE AND SAFEGUARD ITS SYSTEMS AND DATA. HONEYWELL SHALL HAVE NO LIABILITY FOR (I) CUSTOMER'S FAILURE TO IMPLEMENT THE RECOMMENDED UPDATES OR ACTIONS OR (II) CUSTOMER'S FAILURE TO SECURE AND **SAFEGUARD ITS SYSTEMS AND DATA. SUCH FAILURES CAN VOID HONEYWELL'S WARRANTY OBLIGATIONS.**
- YOUR USE OF THE INFORMATION ON THIS DOCUMENT OR MATERIALS LINKED FROM THIS DOCUMENT IS AT YOUR OWN RISK.
- HONEYWELL RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME AND WITHOUT NOTICE.
- HONEYWELL PROVIDES THE CVSS SCORES "AS IS" WITHOUT WARRANTY OF ANY KIND. HONEYWELL DISCLAIMS THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PURPOSE AND MAKES NO EXPRESS WARRANTIES EXCEPT AS MAY BE STATED IN A WRITTEN AGREEMENT WITH AND FOR ITS CUSTOMERS

Honeywell

- IN NO EVENT WILL HONEYWELL BE LIABLE TO ANYONE FOR ANY DIRECT, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES.