Honeywell

SECURITY NOTICE

SN2026-06-25 #01: Time-of-Use Signature Bypass in Honeywell IQ Multi Access IN HONEYWELL IQ Multi Access – (CVE-2026-13742)

This article contains:

It applies to:
IQ Multi Access Version V27and V28

Skills prerequisite:
Qualified personnel with administrative credentials etc.

Executive Summary

Honeywell is aware of vulnerabilities Time-of-Use Signature Bypass in IQ Multi Access Version V27 and V28.

This vulnerability about lack of digital signature verification before execution of downloaded content could allow local attacker to potentially exploit this vulnerability, leading to the replacement of downloaded file with a malicious one. This issue has been assigned CVE-2026-13742 and rated with a severity of Medium. Honeywell strongly recommends that users upgrade to the version identified below to resolve the vulnerability.

Vulnerability Synopsis

1. Time-of-Use Signature Bypass in Honeywell IQ Multi Access – (CVE-2026-13742)
   Lack of signature verification before execution of downloaded content

CVSS Base Score: 5.9 (Medium)

CVSS Vector:

https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:L/AC:H/AT:P/PR:L/UI:N/VC:L/VI:H/VA:H/SC:N/SI:N/SA:N

CVE Number: CVE-2026-13742

Honeywell

Technical Summary

Honeywell IQ Multi Access performs signature verification only during the download phase but not re-validating the integrity and authenticity of the file prior to execution. This creates a time-of-check to time-of-use (TOCTOU) window where the file can be modified or replaced by an attacker, leading to execution of untrusted code.

Mitigation

See Remediation section below.

Affected Products

Product(s)/ Component(s)	CVE	Advisory/Update
IQ Multi Access	**CVE-2026-13742**	Link to patch

Remediation

Honeywell Product Security strongly recommends affected customers to update their affected products once the update is available.

Honeywell

Subscribe to Automated Emails

You may subscribe to the GTAC Knowledge Sharing Mails which provides users with valuable tips & tricks, lessons learned and recommendations on a regular basis.

Further support required?

If you have any questions concerning this notification, please contact your local Honeywell office or the HPS Technical Support Center. Visit process.honeywell.com and select "Contact Us" for country-specific customer contact numbers.

Further support required?

If you have any questions concerning this notification, please contact PSIRT@Honeywell.com. Visit Product Security (honeywell.com) to view all Honeywell's Security Notices.

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