

PRODUCT BULLETIN

Date	15/09/2026
PRODUCTS AFFECTED	
Part Number	Various
Description	Hikvision Security vulnerability disclosure
ISSUE	Hikvision publicly disclosed three vulnerabilities affecting certain Intercom products, HikCentral Access Control versions and Wi-Fi cameras. Please find the attached Partner Letter for further information. Hikvision has already released firmware/software updates to address all three vulnerabilities. At this stage, Hikvision is not aware of these vulnerabilities being exploited in the field. For more details, please refer to the relevant Hikvision Security Advisories.
DETAIL	The newly disclosed vulnerabilities affect certain Hikvision Intercom products, HikCentral Access Control versions and Wi-Fi cameras. Considering the products used in the ANZ market and the prerequisites required for exploitation, the overall practical risk to the ANZ market is considered low and manageable. Hikvision has released firmware/software updates for all three vulnerabilities. At this stage, Hikvision is not aware of these vulnerabilities being exploited in the field. Firmware/software upgrades are not considered necessary for products currently held in distributor inventory. HikCentral Access Control is not used in the ANZ region and therefore has no impact on the ANZ market; Wi-Fi camera sales in the ANZ region are very limited, and exploitation of the vulnerability requires valid account credentials; The Intercom vulnerability may allow access cards to be duplicated. However, exploitation requires physical access to the user's card, as well as the necessary hardware and software tools for card duplication, making exploitation relatively difficult.
REMEDY	As per the following table.

www.ness.com.au

Ness Corporation Pty Ltd ABN 28 069 984 372 Private Bag 23 Seven Hills NSW 1730 Australia Ph +61 2 8825 9222 Fax +61 2 9838 8508 Email: ness@ness.com.au



Quality
ISO 9001
NSW Head Office only

Sydney
4 / 167 Prospect Hwy
Seven Hills NSW 2147
Phone 02 8825 9222
Fax 02 9674 2520
sales@ness.com.au

Melbourne
4 / 56 Norcal Rd
Nunawading VIC 3131
Phone 03 9875 6400
nessmelb@ness.com.au

Brisbane
Unit 5 / 16 Metroplex Ave
Murarrie QLD 4172
Phone 07 3399 4910
nessbris@ness.com.au

Adelaide
Unit 1 / 22 Ware St
Thebarton SA 5031
Phone 08 8152 0000
adelaide@ness.com.au

Perth
1 / 9 Inverness St
Malaga WA 6090
Phone 08 9328 2511
nessper@ness.com.au

PRODUCT BULLETIN

CVE Number & Risk Score	Main Affected Products	Vulnerability Description	Hikvision ANZ Evaluation	Hikvision ANZ Action Plan
CVE-2026-85544 CVSS 5.2 – Medium	Some Hikvision Intercom Products	Under certain conditions, the vulnerability may allow an attacker to duplicate an access card.	Exploitation requires the attacker to physically obtain the user's access card , as well as possess the necessary hardware and software tools for card duplication . Considering these prerequisites, the practical exploitation barrier is relatively high.	Relevant customers using affected products are encouraged to upgrade to the fixed firmware.
CVE-2026-85545 CVSS 7.1 – High	HikCentral Access Control	Vulnerability affecting certain versions of HikCentral Access Control.	HikCentral Access Control is not used in the ANZ region. Therefore, there is no practical impact to the ANZ market.	No ANZ action required.
CVE-2026-85543 CVSS 4.3 – Medium	Some Hikvision Wi-Fi Cameras	An authenticated low-privilege user may potentially obtain device Wi-Fi configuration information.	Wi-Fi camera sales and deployments in ANZ are very limited . Exploitation also requires the attacker to already possess valid account credentials and authenticate to the device. Therefore, the practical exposure in ANZ is considered low.	Relevant customers using affected products are encouraged to upgrade to the fixed firmware.

www.ness.com.au

Ness Corporation Pty Ltd ABN 28 069 984 372 Private Bag 23 Seven Hills NSW 1730 Australia Ph +61 2 8825 9222 Fax +61 2 9838 8508 Email: ness@ness.com.au



Quality
ISO 9001
NSW Head Office only

Sydney
4 / 167 Prospect Hwy
Seven Hills NSW 2147
Phone 02 8825 9222
Fax 02 9674 2520
sales@ness.com.au

Melbourne
4 / 56 Norcal Rd
Nunawading VIC 3131
Phone 03 9875 6400
nessmelb@ness.com.au

Brisbane
Unit 5 / 16 Metroplex Ave
Murarrie QLD 4172
Phone 07 3399 4910
nessbris@ness.com.au

Adelaide
Unit 1 / 22 Ware St
Thebarton SA 5031
Phone 08 8152 0000
adelaide@ness.com.au

Perth
1 / 9 Inverness St
Malaga WA 6090
Phone 08 9328 2511
nessper@ness.com.au



September 15, 2026

Dear Valued Partner:

Today, Hikvision publicly disclosed three previously unknown vulnerabilities.

A Vulnerability in Some Hikvision Intercom Products

Hikvision disclosed a vulnerability (CVE-2026-85544) in some Hikvision Intercom Products. The company has issued updated firmware, available on our [website](#), to address this vulnerability.

Hikvision has rated this vulnerability as 5.2 using the [CVSS v3.1 calculator](#). The list of affected products and technical details of the vulnerability can be found in our [security advisory](#). Please check the advisory to learn the technical details.

This vulnerability was reported to the Hikvision Security Response Center (HSRC) by an independent security researcher Filipe Moreira, and Hikvision has been actively working with the researcher to patch and verify the successful mitigation.

A Vulnerability in Some HikCentral Access Control Versions

Hikvision disclosed a vulnerability (CVE-2026-85545) in some HikCentral Access Control versions. The company has released an update ([V2.5.1](#)) to fix this vulnerability.

Hikvision has rated this vulnerability as 7.1 using the [CVSS v3.1 calculator](#). The versions affected by the vulnerability are listed in our [security advisory](#).

This vulnerability was reported to the Hikvision Security Response Center (HSRC) by Patrick Tung (@patrickt2017), and Hikvision has been actively working with the researcher to patch and verify the successful mitigation.

A Vulnerability in Some Hikvision Wi-Fi Cameras

Hikvision disclosed a vulnerability (CVE-2026-85543) in some Hikvision Wi-Fi cameras. Due to insufficient privilege validation on certain interfaces, an authenticated user with low privileges could potentially obtain device Wi-Fi configuration information. The company has issued updated firmware, available on our [official website](#), to address this vulnerability, with details included in the [release note](#).

Hikvision has rated this vulnerability as 4.3 using the [CVSS v3.1 calculator](#). The list of affected products can be found in the release note. Users are strongly recommended to upgrade their devices to mitigate this issue.



With this letter, we want to reassure you of Hikvision's strong commitment to cybersecurity by following the standard Coordinated Disclosure Process. While Hikvision is not aware of these vulnerabilities being exploited in the field, we encourage our partners to work with their customers, following the guidance provided in the advisory to ensure proper cyber hygiene.

Hikvision is a CVE Partner and is committed to continuing to work with third-party security researchers to find, patch, disclose and release updates to products in a timely manner that best protects the users of Hikvision products. To report any security issues or vulnerabilities in Hikvision products and solutions, please contact the Hikvision Security Response Center at hsrc@hikvision.com. On our [website](#), Hikvision discloses the vulnerabilities and informs about the remediation in a transparent and responsible manner.

Hikvision strictly complies with the laws and regulations in all countries and regions where we operate and our efforts to ensure the security of our products go beyond what is mandated.

Please do not hesitate to contact our team with any questions or concerns.

Kind Regards,

A handwritten signature in black ink, appearing to read "Carmelo Zheng", with a stylized flourish at the end.

Carmelo Zheng
CEO
Hikvision Oceania