16th June 2023
Dear Valued Partner,

Some vulnerabilities were reported to Hikvision by Andres Hinnosaar with the support of NATO CCDCOE and Peter Szot from Skylight Cyber. Hikvision has issued patches available on our website to fix the vulnerabilities. Please check the following details.

- Vulnerability with CVE ID CVE-2023-28809

Some access control products are potentially affected. This vulnerability can only be exploited for unauthorized access when the following four conditions occur at the same time:

- ❖ Get the correct password
- ❖ Get the correct IP address
- ❖ When the authorised user is logging in to the device
- ❖ Get the session ID

It is extremely challenging for a hacker to exploit this vulnerability for unauthorized access because it is difficult for all of the above four conditions to occur simultaneously. We have conducted multiple tests in the laboratory and have not been able to reproduce this issue yet.

- Vulnerability with CVE ID CVE-2023-28810

Some access control and intercom products are potentially affected. Only when the unauthorised user physically connects the laptop or PC to the switch or router can this vulnerability be exploited to change the IP settings, such as the IP address, gateway, and network mask.
Other parameters cannot be modified, and the device will not be taken over by the hacker. This means that visitors may not be able to use the door station to call the indoor station and may not be able to use the lift. However, the residents can still use a card or pin code to open the door through the door station or use the lift.
It is not feasible to exploit this vulnerability through the internet, which makes it extremely difficult to do so.

Hikvision Oceania
Headquarters: 46 Brookhollow Ave, Baulkham Hills, New South Wales 2153, Australia
Main: +61 1300 557 450 / +64 (0) 92173127
Tech Support Line: +61 1300 976 305
Sales Email: sales.au@hikvision.com / sales.nz@hikvision.com
Website: www.hikvision.com/au-en/

Affected Devices

Access Control	CVE ID	Affected Firmware Versions
DS-K1T804AXX	CVE-2023-28809 CVE-2023-28810	Versions below V1.4.0_build221212 (including V1.4.0_build221212)
DS-K1T341AXX		Versions below V3.2.30_build221223 (including V3.2.30_build221223)
DS-K1T671XXX		Versions below V3.2.30_build221223 (including V3.2.30_build221223)
DS-K1T343XXX		Versions below V3.14.0_build230117 (including V3.14.0_build230117)
DS-K1T341C		Versions below V3.3.8_build230112 (including V3.3.8_build230112)
DS-K1T320XXX		Versions below V3.5.0_build220706 (including V3.5.0_build220706)

Intercom	CVE ID	Affected Versions
DS-KH63xx Series DS-KH85xx Series	CVE-2023-28810	Versions below V2.2.8_build230219 (including V2.2.8_build230219)
DS-KH9310-WTE1(B) DS-KH9510-WTE1(B)		Versions below V2.1.76_build230204 (including V2.1.76_build230204)

We recommend that actions be taken to mitigate potential risks. Please ensure the following hardening practices are employed to provide additional resilience for your customers.

1. Go to the Hikvision website to search for the latest firmware, and then upgrade the firmware.
2. As always, password strength is critical. Ensure your customers set up complex passwords containing letters (uppercase and lowercase), numbers, and special characters.

If you require assistance, don't hesitate to contact Hikvision Support at 1300976305 or email techsupportau@hikvision.com.

Hikvision Oceania
Headquarters: 46 Brookhollow Ave, Baulkham Hills, New South Wales 2153, Australia
Main: +61 1300 557 450 / +64 (0) 92173127
Tech Support Line: +61 1300 976 305
Sales Email: sales.au@hikvision.com / sales.nz@hikvision.com
Website: www.hikvision.com/au-en/