

# CVE-2017-7921

## Hikvision Multiple Products Improper Authentication Vulnerability

Exigent

CISA KEV since Mar 5, 2026

Actively exploited

Public exploit module (Metasploit)

An Improper Authentication issue was discovered in Hikvision DS-2CD2xx2F-I Series V5.2.0 build 140721 to V5.4.0 build 160530, DS-2CD2xx0F-I Series V5.2.0 build 140721 to V5.4.0 Build 160401, DS-2CD2xx2FWD Series V5.3.1 build 150410 to V5.4.4 Build 161125, DS-2CD4x2xFWD Series V5.2.0 build 140721 to V5.4.0 Build 160414, DS-2CD4xx5 Series V5.2.0 build 140721 to V5.4.0 Build 160421, DS-2DFx Series V5.2.0 build 140805 to V5.4.5 Build 160928, and DS-2CD63xx Series V5.0.9 build 140305 to V5.3.5 Build 160106 devices.

EVRS

90/100

Immediate priority

CVSS V3.1

9.8

Critical · NVD

EPSS

0.999

99.99th percentile · FIRST

CISA DEADLINE

Mar 26, 2026

CISA federal deadline · Overdue by 7 months

### Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

|                                              |                                          |                                                         |                                        |
|----------------------------------------------|------------------------------------------|---------------------------------------------------------|----------------------------------------|
| <input checked="" type="checkbox"/> CISA KEV | Listed in the catalog                    | <input type="checkbox"/> Vendor exploitation            | Confirmed exploitation in the wild     |
| <input type="checkbox"/> Ransomware          | No known ransomware campaign association | <input type="checkbox"/> KEV recency                    | Added to CISA KEV within the last year |
| <input checked="" type="checkbox"/> EPSS     | 0.999 probability                        | <input type="checkbox"/> Pre-patch disclosure           | Disclosure status unavailable          |
| <input checked="" type="checkbox"/> CVSS     | Base score 9.8                           | <input type="checkbox"/> Microsoft Exploitability Index | Not a Microsoft CVE                    |

### Remediation

**Out-of-band / urgent** Patch or fixed version identified

**CISA required action:** Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

The improper authentication vulnerability occurs when an application does not adequately or correctly authenticate users. This may allow a malicious user to escalate his or her privileges on the system and gain access to sensitive information.

### Affected and fixed versions · 108 more affected products on the NVD record

| PACKAGE                       | AFFECTED | FIXED IN                | SOURCE |
|-------------------------------|----------|-------------------------|--------|
| ds-2cd2032-i firmware         | —        | no fixed version listed | NVD    |
| ds-2cd2112-i firmware         | —        | no fixed version listed | NVD    |
| ds-2cd2132-i firmware         | —        | no fixed version listed | NVD    |
| ds-2cd2212-i5 firmware        | —        | no fixed version listed | NVD    |
| ds-2cd2232-i5 firmware        | —        | no fixed version listed | NVD    |
| ds-2cd2312-i firmware         | —        | no fixed version listed | NVD    |
| ds-2cd2332-i firmware         | —        | no fixed version listed | NVD    |
| ds-2cd2412f-i\(\w\\) firmware | —        | no fixed version listed | NVD    |

## Sources

**Vendor guidance** [github.com/advisories/GHSA-82r9-7ww3-jr86](https://github.com/advisories/GHSA-82r9-7ww3-jr86)

**hikvision.com** [hikvision.com/us-en/support/document-center/special-notices/privilege-escalating-vulnerability-in-certain-hikvision-ip-cameras/](https://hikvision.com/us-en/support/document-center/special-notices/privilege-escalating-vulnerability-in-certain-hikvision-ip-cameras/)  
**CISA KEV** [cisa.gov/known-exploited-vulnerabilities-catalog](https://cisa.gov/known-exploited-vulnerabilities-catalog)  
**Current data** [evulnable.com/vulnerability-management/cve/CVE-2017-7921](https://evulnable.com/vulnerability-management/cve/CVE-2017-7921)

**NVD** [nvd.nist.gov/vuln/detail/CVE-2017-7921](https://nvd.nist.gov/vuln/detail/CVE-2017-7921)

**ENISA EUVD** [euvd.enisa.europa.eu/vulnerability/EUVD-2017-16892](https://euvd.enisa.europa.eu/vulnerability/EUVD-2017-16892)

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.