

CVE-2021-36260

Hikvision Improper Input Validation

Exigent

CISA KEV since Jan 10, 2022

Actively exploited

Public exploit module (Metasploit)

A command injection vulnerability in the web server of some Hikvision product. Due to the insufficient input validation, attacker can exploit the vulnerability to launch a command injection attack by sending some messages with malicious commands.

EVRS 87 / 100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.999 99.96th percentile · FIRST	CISA DEADLINE Jan 24, 2022 KEV since 2022 · listed over a year
--	--	---	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.999 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

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

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions · 504 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
ds-2cd2026g2-iu\sl firmware	—	no fixed version listed	NVD
ds-2cd2046g2-iu\sl firmware	—	no fixed version listed	NVD
ds-2cd2066g2-i(u\) firmware	—	no fixed version listed	NVD
ds-2cd2066g2-iu\sl firmware	—	no fixed version listed	NVD
ds-2cd2086g2-i(u\) firmware	—	no fixed version listed	NVD
ds-2cd2086g2-iu\sl firmware	—	no fixed version listed	NVD
ds-2cd2166g2-i(su\) firmware	—	no fixed version listed	NVD
ds-2cd2186g2-i(su\) firmware	—	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-v276-9v2g-hx55

Additional guidance hikvision.com/en/support/cybersecurity/security-advisory/security-notification-command-injection-vulnerability-in-some-hikvision-products/cisa.gov/known-exploited-vulnerabilities-catalog

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

Current data evulnable.com/vulnerability-management/cve/CVE-2021-36260

NVD nvd.nist.gov/vuln/detail/CVE-2021-36260

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2021-22880

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