OUTBREAK ALERTS

Hikvision IP Cameras Command Injection Vulnerability

A Command Injection vulnerability in the web server of some Hikvision products.

https://www.hikvision.com/en/support/cybersecurity/security-advisory/security-notification-command-injection-vulnerability-in-some-hikvision-products/

CVEs: CVE-2021-36260

Due to the insufficient input validation, an attacker can exploit the vulnerability to launch a command injection attack by sending crafted messages with malicious commands.

Background	Hikvision is a leading provider of IoT sensor technologies such as IP cameras used by retail, energy, educational and military sectors. Back in December 2021, Fortinet posted a blog about this vulnerability on how attackers can take advantage of it. For more information, refer to the additional resources.
Announced	Sep 26, 2021: Security notification by vendor.
Latest Developments	Aug 26, 2022: Tens of thousands of Hikvision IP cameras are still vulnerable to a critical, 11-month-old CVE, leaving thousands of organizations exposed. A recent research shows multiple hacking groups collaborating on exploiting Hikvision IP cameras using the command injection vulnerability (CVE-2021-36260) globally. FortiGuard Labs is seeing active exploitation attempts since the release of IPS signature back in Oct, 2021 and a significant uptick in the last 3 months.

Cyber Kill Chain

Reconnaissance

FortiDeceptor
Decoy VM 3.3+

Weaponization

Delivery

Exploitation

FortiGate
IPS 18.192
Blocks attack attempts related to Hikvision IP Cameras (CVE-2021-36260)

FortiWeb
Web App Security 0.00328
Blocks attack attempts related to Hikvision IP Cameras (CVE-2021-36260)

FortiSASE
IPS 18.192
Blocks attack attempts related to Hikvision IP Cameras (CVE-2021-36260)

FortiNDR
IPS 18.192
Blocks attack attempts related to Hikvision IP Cameras (CVE-2021-36260)

FortiADC
IPS 18.192
Blocks attack attempts related to Hikvision IP Cameras (CVE-2021-36260)

Web App Security 1.00037
Blocks attack attempts related to Hikvision IP Cameras (CVE-2021-36260)

FortiProxy
IPS 18.192
Blocks attack attempts related to Hikvision IP Cameras (CVE-2021-36260)

Installation

C2

Action

Endpoint

Incident Response (Security Operations)

To help customers identify and protect vulnerable, FortiAnalyzer, FortiSIEM and FortiSOAR updates are available to raise alerts and escalate to incident response:

FortiGate	***IoT/IIoT Detection*** Version 7.2.1 https://community.fortinet.com/t5/FortiGate/Technical-Tip-Using-FortiGate-to-detect-Hikvision-IP-Cameras/ta-p/222299
FortiAnalyzer	***Outbreak Detection*** Version 1.060 https://www.fortiguard.com/updates/outbreak-detection-service?version=1.00060 ***Threat Hunting*** Version 7.0 https://community.fortinet.com/t5/FortiAnalyzer/Technical-Tip-Using-FortiAnalyzer-to-detect-Hikvision-IP-Cameras/ta-p/222291
FortiSIEM	***Content Update*** Version 303 https://help.fortinet.com/fsiem/6-6-0/Online-Help/HTML5_Help/content_updates.htm#Content3 ***Threat Hunting*** Version 6.4.0+ https://community.fortinet.com/t5/FortiSIEM/Technical-Tip-Using-FortiSIEM-to-detect-Hikvision-IP-Cameras/ta-p/223655

Additional Resources

NIST	https://nvd.nist.gov/vuln/detail/CVE-2021-36260
Fortinet Blog	https://www.fortinet.com/blog/threat-research/mirai-based-botnet-moobot-targets-hikvision-vulnerability
Threat Post	https://threatpost.com/cybercriminals-are-selling-access-to-chinese-surveillance-cameras/180478/
The Dark Reading	https://www.darkreading.com/vulnerability-management/thousands-organizations-risk-critical-ip-camera-bug
The Record Media	https://therecord.media/experts-warn-of-widespread-exploitation-involving-hikvision-cameras/
Cyfirma	https://www.cyfirma.com/wp-content/uploads/2022/08/HikvisionSurveillanceCamerasVulnerabilities.pdf