FORTINET

FortiGuard Labs 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.

Latest Developments

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 few months.

- December 06, 2021: FortiGuard Labs release a Threat blog on Mirai based botnet moobot targeting Hikvision vulnerability.
  https://www.fortinet.com/blog/threat-research/mirai-based-botnet-moobot-targets-hikvision-vulnerability
- December 16, 2024: The Federal Bureau of Investigation (FBI) released this Private Industry Notification (PIN) to highlight HiatusRAT scanning campaigns against Chinese-branded web cameras and DVRs.
  https://www.ic3.gov/CSA/2024/241216.pdf
- September 26, 2021: Security notification released by the vendor

PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

Decoy VM

FortiDeceptor
v3.3+

IPS

Detects and blocks attack attempts leveraging the vulnerability

FortiADC	FortiGate	FortiNDR	FortiProxy	FortiSASE
DB 18.192	*DB 18.192*	*DB 18.192*	*DB 18.192*	*DB 18.192*

Web App Security

Detects and blocks attack attempts leveraging the vulnerability

FortiADC	FortiWeb
DB 1.00037	*DB 0.00328*

DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

IOC

FortiAnalyzer	FortiSOCaaS	FortiSIEM	FortiSOAR

Outbreak Detection

FortiAnalyzer	FortiSIEM
DB 1.00060	*DB 303*

Threat Hunting

FortiAnalyzer	Lacework CNAPP	FortiClient	FortiEDR	FortiNDR Cloud	FortiSIEM
v6.4+	*v7.0+*	*v7.0+*	*v7.0+*	*v7.0+*	*v6.4+*

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automatically respond to this outbreak.

FortiXDR

Assisted Response Services

Experts to assist you with analysis, containment and response activities.

Incident Response

RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

NOC/SOC Training

Train your network and security professionals and optimize your incident response to stay on top of the cyberattacks.

NSE Training | Response Readiness

End-User Training

Raise security awareness to your employees that are continuously being targeted by phishing, drive-by download and other forms of cyberattacks.

Security Awareness & Training

InfoSec Services

Security readiness and awareness training for SOC teams, InfoSec and general employees.

Response Readiness

IDENTIFY

Identify processes and assets that need protection:

Attack Surface Hardening

Check Security Fabric devices to build actionable configuration recommendations and key indicators.

Security Rating

Attack Surface Monitoring (Inside & Outside)

Security reconnaissance and penetration testing services, covering both internal & external attack vectors, including those introduced internally via software supply chain.

Security Rating

Additional Resources

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

Learn more about FortiGuard Outbreak Alerts

FortiGuard Labs

FORTINET