



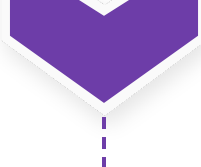
# Hikvision IP Cameras Command Injection Vulnerability

## 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 released by the vendor  Dec 06, 2021: Mirai-based Botnet - Moobot Targets Hikvision Vulnerability, Threat Analysis by Fortinet <a href="https://www.fortinet.com/blog/threat-research/mirai-based-botnet-moobot-targets-hikvision-vulnerability">https://www.fortinet.com/blog/threat-research/mirai-based-botnet-moobot-targets-hikvision-vulnerability</a>
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 few months.



## PROTECT

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

### Reconnaissance

Decoy VM



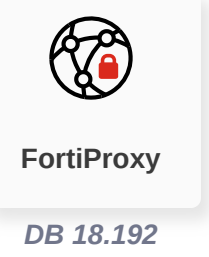
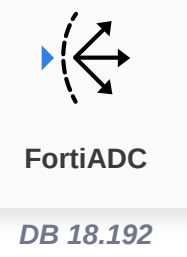
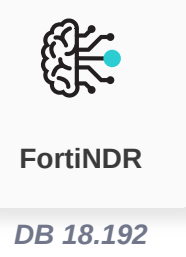
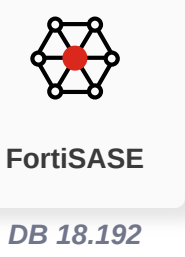
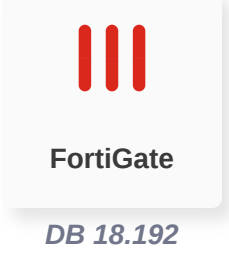
### Weaponization

### Delivery

### Exploitation

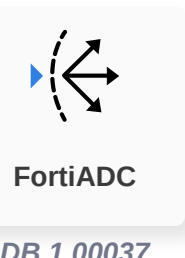
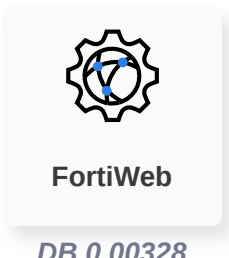
IPS

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



Web App Security

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



### Installation

### C2

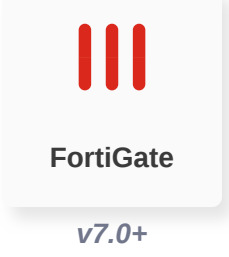
### Action



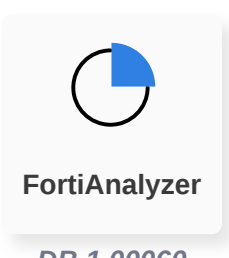
## DETECT

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

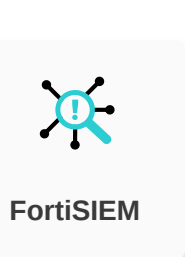
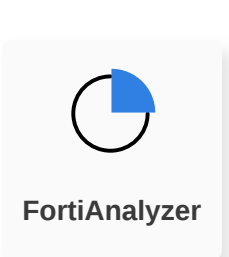
IoT/IIoT Detection



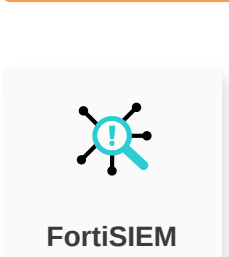
Outbreak Detection



Threat Hunting



Content Update

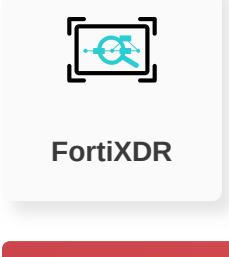


## RESPOND

Develop containment techniques to mitigate impacts of security events:

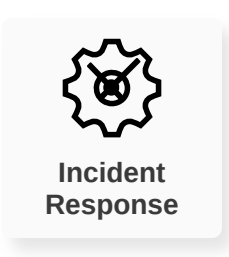
Automated Response

Services that can automatically respond to this outbreak.



Assisted Response Services

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



## RECOVER

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

InfoSec Services

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



## IDENTIFY

Identify processes and assets that need protection:

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.



## Additional Resources

Fortinet Blog	<a href="https://www.fortinet.com/blog/threat-research/mirai-based-botnet-moobot-targets-hikvision-vulnerability">https://www.fortinet.com/blog/threat-research/mirai-based-botnet-moobot-targets-hikvision-vulnerability</a>
Threat Post	<a href="https://threatpost.com/cybercriminals-are-selling-access-to-chinese-surveillance-cameras/180478/">https://threatpost.com/cybercriminals-are-selling-access-to-chinese-surveillance-cameras/180478/</a>
Dark Reading	<a href="https://www.darkreading.com/vulnerability-management/thousands-organizations-risk-critical-ip-camera-bug">https://www.darkreading.com/vulnerability-management/thousands-organizations-risk-critical-ip-camera-bug</a>
The Record Media	<a href="https://therecord.media/experts-warn-of-widespread-exploitation-involving-hikvision-cameras/">https://therecord.media/experts-warn-of-widespread-exploitation-involving-hikvision-cameras/</a>

Learn more about [FortiGuard Outbreak Alerts](#)

