



---

December 31, 2024

CYBERSECURITY

---

## Topic: Vulnerability-FortiOS VPN SSL

### Overview :

A security was published in December 2022 on the product FortiOS SSL-VPN by the fortinet company (CVE-2022-42475). This is about a heap-based buffer overflow that may allow a remote unauthenticated attacker to execute arbitrary code or commands vis speciaficly crafted requests. Remediation based on firmware upgrades were published by Fortinet.

However, some intelligence teams report that cyber attacks using this weakness seems to be deployed.

According to recent news from the Dutch Military Intelligence and Security Service, a threat actor may have compromised nearly 20,000 Fortigate appliances worldwide.

- The threat actor has installed a backdoor dubbed “COATHANGER” at relevant targets worldwide. In this way, the threat actor gained permannet access to the compromised systems.
- This backdoor has the ability to persist even after the equipment has been patched following the compromise.
- A technical incident analysis has been published by fortinet with detailed IoCs.
- The national cuber Security center of netherlands and the Dutch Military Intelligence and Security Service have published a technical report on the “COATHANGER” remote access trojan.

### ❖ Technical Incident analysis

[Analysis of FG-IR-22-398 – FortiOS - heap-based buffer overflow in SSLVPNd | Fortinet Blog](#)

### ❖ Netherland Publication NCSC (09/02/2024)

<https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2024/februari/6/mivd-avid-advisory-coathanger-tlp-clear/TLP-CLEAR+MIVD+AIVD+Advisory+COATHANGER.pdf>

## Affected Components

- FortiGate FG100x (x=D, E, F, G)
- FortiGate FG60x (x=D, E, F, G)
- FortiGate FG301x (x=D, E, F, G)

## Affected Firmware

- FortiOS version 7.2.0 through 7.2.2
- FortiOS version 7.0.0 through 7.0.8
- FortiOS version 6.4.0 through 6.4.10
- FortiOS version 6.2.0 through 6.2.11

- FortiOS version 6.0.0 through 6.0.15
- FortiOS version 5.6.0 through 5.6.14
- FortiOS version 5.4.0 through 5.4.13
- FortiOS version 5.2.0 through 5.2.15
- FortiOS version 5.0.0 through 5.0.14

GE Vernova has identified that the following one main product(s) or service(s) that are potentially impacted.

**Impacted Solutions Products**

- Any network communication link using the SSL VPN service of FortiGate security appliances (e.g. Firewall FG 100, FG 60, FG 301)

**Identified Risks**

<b>CVE-2022-42475</b>	Vulnerability Details: Out-of-bound read/write vulnerability	CVSSv3 Score: 9.8 (Critical)
-----------------------	---	---------------------------------

COATHANGER gains its initial access by exploiting the vulnerability identified as CVE-2022-42475. This flaw provides the perfect entry point for threat actors, allowing them to install the malicious software on the FortiGate appliance without detection. Once inside, the malware opens the door for complete access by the attackers, putting sensitive information and network security at grave risk. If successfully exploited this flaw could allow a remote unauthenticated attacker to execute arbitrary code leading to a complete takeover of a vulnerable system.

The COATHANGER malware is stealthy and persistent. It hides itself by hooking system calls that could reveal its presence. It can survive reboots and firmware upgrades.

**Mitigation**

Fortinet supplier recommends taking immediate action to mitigate this threat by disabling SSL VPN and by performing the update of the FortiGate appliance firmware to the latest release, as documented in its remediation part.

The solution given by the supplier is the upgrade of the product:

- Please upgrade to FortiOS version 7.2.3 or above
- Please upgrade to FortiOS version 7.0.9 or above
- Please upgrade to FortiOS version 6.4.11 or above
- Please upgrade to FortiOS version 6.2.12 or above

- Please upgrade to FortiOS version 6.0.16 or above

In addition to that and as a minimum, GE Vernova recommends, to follow the instructions provided by Fortinet supplier to search for indicators of compromise, as documented in the following technical articles & suggestions.

These articles describe the forensic process enabling to detect the “COATHANGER” threat.

<https://community.fortinet.com/t5/FortiGate/Technical-Tip-FortiGate-Forensic-Image-to-detect-Coathanger/ta-p/327803>

<https://community.fortinet.com/t5/FortiGate/Technical-Tip-Critical-vulnerability-Protect-against-heap-based/ta-p/239420>

It’s important to note, even if the vendor’s mitigations provide information on the possible risk of compromise, this cannot be considered sufficient to guarantee the total innocuity of the customer’s system against the cyber-menace. No detection of the “COATHANGER” threat using the Fortinet proposed means, should NOT be considered as a “no compromission situation” in customer risk analysis.

As a mitigation, to contain the risk, other security measures shall be considered to monitor traffic and connection to the equipment.

### **Remediation**

Customer must be aware that here leaning on firmware updates could not be considered sufficient if the considered process control system is a critical asset for its business. In this case, best practices recommend the replacement of the hardware equipment with a similar new one supplied from a legitimate source to guarantee an acceptable level of the security of the infrastructure.

### **Defense-in-depth**

To minimize the risk of the exploitation of current and future system vulnerabilities, GE Vernova highly recommends implementation of a defense-in-depth strategy (complementary defenses in Physical, Technical, and administrative domains) for your critical process control systems.

We will be pleased to support you in the enhancement of your cybersecurity strategy and improve or update your current equipment with latest cybersecurity methodologies and solutions. We suggest that a thorough analysis of your cybersecurity status be performed and resulting recommendations for an optimal solution be implemented according to the level of risk exposure and/or the standard frameworks which are applicable to your needs.

Contact your GE Vernova salesperson or our Help Desk for help with ordering cybersecurity services and solutions.

**Helpdesk e-mail: [helpdeskEU.steampower@ge.com](mailto:helpdeskEU.steampower@ge.com)**

**Hotline phone number: +48 539 192 401**

**Solene Barnes**

Product Security Manager, GE Vernova – Steam Power

**Revision History**

<b>Version</b>	<b>Release Date</b>
A	Dec, 31 2024