arabelle solutions
EDF GROUP

November 20, 2024 **CYBERSECURITY**

Topic: Vulnerability-FortiOS VPN SSL

Overview:

A security alert 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 via specifically 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 permanent 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 Cyber 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:** https://www.fortinet.com/blog/psirt-blogs/analysis-of-fg-ir-22-398-fortios-heap-based-buffer-overflow-in-sslvpnd

- **NCSC Netherland publication (09/02/2024):** https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2024/februari/6/mivd-aivd-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

Arabelle Solutions has identified that the following one main product(s) or service(s) that are potentially impacted

Impacted Arabelle Solutions Products:

- Any network communication link using the SSL VPN service of FortiGate security appliances (e.g. firewall FG 100, FG60, FG301)

Identified risks:

CVE-2022-42475 - Vulnerability Details – Out-of-bounds 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 survives 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 of that and as a minimum, Arabelle Solutions recommends to follow instructions provided by Fortinet supplier to search for indicators of compromise, as documented in the following Technical Tips.

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 that, even if the vendor’s mitigations provide information on the possible risk of compromission, this can not be considered sufficient to guarantee the total innocuity of the customer’s system against this 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 rely 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 brand 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, Arabelle Solutions 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 Arabelle Solutions Automation & Controls Sales person or our Help Desk at +33 1 60 13 43 91 /
helpdesk.control-systems@arabellesolutions.com for help with ordering cybersecurity services and solutions.

Revision History

Version	Release Date	Purpose
A	November 20, 2024	Initial version