

HiveForce Labs

# THREAT ADVISORY

 **VULNERABILITY REPORT**

## **Critical Vulnerability in FortiOS SSL VPN Exploited in the Wild**

Date of Publication

February 9, 2024

Admiralty Code

A1

TA Number

TA2024053




# Summary

**First Seen:** February 7, 2024

**Affected Platform:** Fortinet FortiOS SSL-VPN

**Impact:** A critical Out-of-Bounds Write vulnerability (CVE-2024-21762) in Fortinet FortiOS SSL-VPN is actively exploited, enabling remote unauthenticated attacker to execute arbitrary code or command via specially crafted HTTP requests.

## CVE

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-21762	Fortinet FortiOS SSL-VPN Out-of-Bounds Write Vulnerability	Fortinet FortiOS SSL-VPN			

## Vulnerability Details

### #1

A critical vulnerability has been discovered in FortiOS SSL VPN, and Fortinet has issued a warning stating that it is being actively exploited in the wild. CVE-2024-21762 is an out-of-bounds write vulnerability with a CVSS score of 9.6. It enables a remote, unauthenticated attacker to execute arbitrary code through specially crafted HTTP requests.

### #2

A similar vulnerability, CVE-2022-42475, unearthed in 2022, was widely exploited by multiple state actors. The Dutch NCSC has recently identified the deployment of a custom-built RAT targeting Fortinet products. Fortinet has released patches for the vulnerability. In cases where immediate patching is unfeasible, organizations may consider disabling the SSL VPN service from FortiOS as a temporary mitigation measure.

# Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-21762	Fortinet FortiOS versions: 7.4.0 through 7.4.2 7.2.0 through 7.2.6 7.0.0 through 7.0.13 6.4.0 through 6.4.14 6.2.0 through 6.2.15 6.0 all versions	cpe:2.3:o:fortinet:fortios:*:*:*:*:*	CWE-787

## Recommendations



**Apply Patches:** Install the patches released by Fortinet promptly to fix the vulnerability. Patching is the most effective long-term solution.



**Disable SSL VPN Service:** If immediate patching is not feasible, consider disabling the SSL VPN service in FortiOS temporarily. This action can help prevent exploitation until patches can be applied.



**Network Segmentation:** Implement network segmentation to limit the reach of potential attackers. This can help contain the impact of any successful exploitation.



**Network Monitoring:** Enhance network monitoring capabilities to detect any suspicious activity or unauthorized access attempts targeting the SSL VPN service.

## Potential MITRE ATT&CK TTPs

<u>TA0002</u> Execution	<u>TA0042</u> Resource Development	<u>T1588</u> Obtain Capabilities	<u>T1203</u> Exploitation for Client Execution
<u>T1588.005</u> Exploits	<u>T1588.006</u> Vulnerabilities		



## Patch Details

Patched versions of Fortinet FortiOS:

Upgrade to 7.4.3 or above

Upgrade to 7.2.7 or above

Upgrade to 7.0.14 or above

Upgrade to 6.4.15 or above

Upgrade to 6.2.16 or above

Workaround:

Disable SSL VPN (disable webmode is NOT a valid workaround)

Link:

<https://fortiguard.fortinet.com/psirt/FG-IR-24-015>



## References

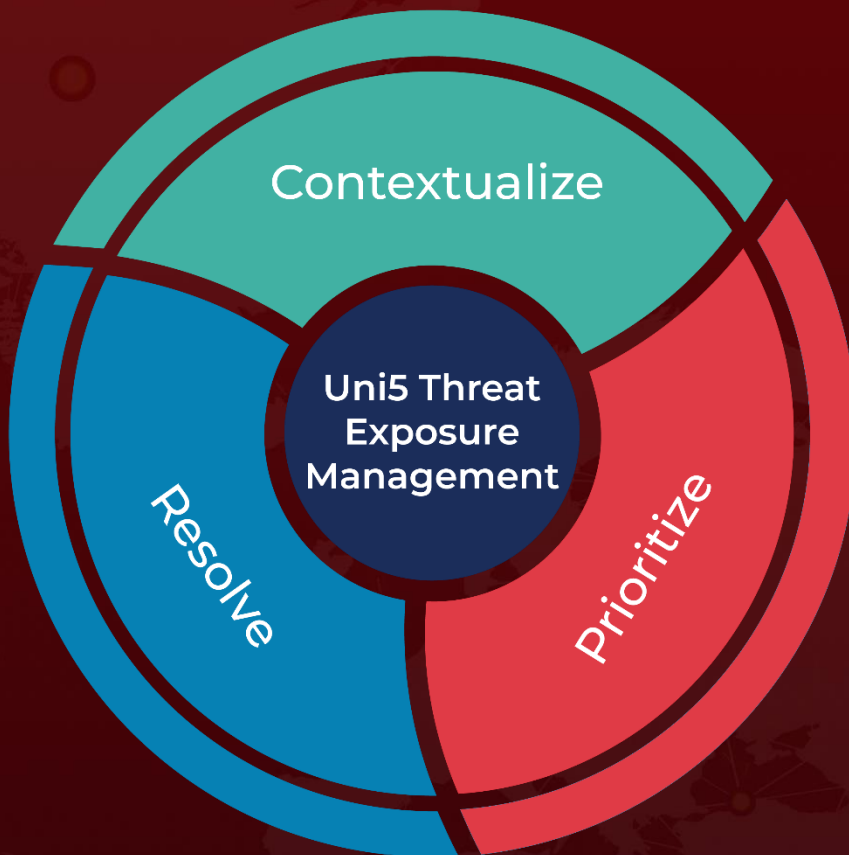
<https://www.csa.gov.sg/alerts-advisories/alerts/2024/al-2024-016>



# What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

**February 9, 2024 • 7:30 AM**

© 2024 All Rights are Reserved by Hive Pro<sup>®</sup>



More at [www.hivepro.com](http://www.hivepro.com)