



Threat Level

 **Red**

 **CISA: AA23-250A**

HiveForce Labs

# THREAT ADVISORY

 **VULNERABILITY REPORT**

## **Nation-State Actors Infiltrate U.S. by Exploiting Zoho and Fortinet Flaws**

Date of Publication

September 8, 2023

Admiralty Code

A1

TA Number

TA2023362

# Summary







**Attack Began:** January 2023

**Targeted Industry:** Aeronautical Sector

**Affected Product:** Zoho ManageEngine, Fortinet FortiOS

**Impact:** Multiple nation-state entities infiltrated a prominent U.S. aeronautics organization by capitalizing on vulnerabilities within Fortinet FortiOS SSL-VPN and Zoho ManageEngine ServiceDesk Plus, subsequently acquiring unauthorized entry and establishing persistence on compromised systems.

## CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2022-47966	Zoho ManageEngine Multiple Products Remote Code Execution Vulnerability	Zoho ManageEngine			
CVE-2022-42475	Fortinet FortiOS Heap-Based Buffer Overflow Vulnerability	Fortinet FortiOS			

# Vulnerability Details

## #1

Multiple state-sponsored entities penetrated a prominent U.S. aerospace organization by exploiting security vulnerabilities within Fortinet FortiOS SSL-VPN and Zoho ManageEngine ServiceDesk Plus. This allowed them to gain illicit access and establish a persistent presence within compromised systems. As early as January 2023, APT actors exploited CVE-2022-47966 to secure initial entry into the organization's web server, which hosted the publicly accessible Zoho ManageEngine ServiceDesk Plus application.

## #2

They ultimately achieved root-level access and created a local user account named 'Azure' with elevated administrative privileges. Subsequently, these actors were capable of downloading malware, conducting network enumeration, harvesting administrative user credentials, and progressing laterally through the organization's network.

## #3

Furthermore, another group of APT actors exploited CVE-2022-42475, effectively leveraging a zero-day vulnerability within Fortinet FortiOS SSL-VPN on the organization's firewall device. These APT actors initiated multiple encrypted sessions using Transport Layer Security (TLS) over Transmission Control Protocol (TCP) port 10443, signifying successful data exchanges originating from the firewall device. Subsequently, they utilized legitimate credentials to pivot from the firewall to a web server, where multiple web shells were deployed.

## Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-47966	Multiple Zoho ManageEngine on-premise <b>products</b>	cpe:2.3:a:zohocorp:manageengine_access_manager_plus:*:*:*:*:*:*:*	CWE-20
CVE-2022-42475	Fortinet <b>FortiOS</b> : 7.2.0 - 7.2.2, 7.0.0 - 7.0.8, 6.4.0 - 6.4.10, 6.2.0 - 6.2.11	cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*	CWE-787

# Recommendations



**Vulnerability Management:** This entails routinely assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security **patches**. Evaluate the security practices of third-party vendors, especially for critical applications and services.



**Access Control and Monitoring:** Implement robust access controls and limit privileges to minimize the potential impact of an attack. Employ monitoring and alerting systems to detect unusual or unauthorized access activities. Continuously monitor for new vulnerabilities and security updates concerning third-party software and dependencies.

# 🕸 Potential MITRE ATT&CK TTPs

<b><u>TA0001</u></b> Initial Access	<b><u>TA0002</u></b> Execution	<b><u>TA0003</u></b> Persistence	<b><u>TA0004</u></b> Privilege Escalation
<b><u>TA0005</u></b> Defense Evasion	<b><u>TA0006</u></b> Credential Access	<b><u>TA0007</u></b> Discovery	<b><u>TA0008</u></b> Lateral Movement
<b><u>TA0009</u></b> Collection	<b><u>TA0011</u></b> Command and Control	<b><u>T1190</u></b> Exploit Public-Facing Application	<b><u>T1059.001</u></b> PowerShell
<b><u>T1053.005</u></b> Scheduled Task	<b><u>T1136.001</u></b> Local Account	<b><u>T1505.003</u></b> Web Shell	<b><u>T1068</u></b> Exploitation for Privilege Escalation
<b><u>T1070.001</u></b> Clear Windows Event Logs	<b><u>T1564.001</u></b> Hidden Files and Directories	<b><u>T1003</u></b> OS Credential Dumping	<b><u>T1049</u></b> System Network Connections Discovery
<b><u>T1040</u></b> Network Sniffing	<b><u>T1570</u></b> Lateral Tool Transfer	<b><u>T1074</u></b> Data Staged	<b><u>T1071.001</u></b> Web Protocols
<b><u>T1219</u></b> Remote Access Software	<b><u>T1571</u></b> Non-Standard Port	<b><u>T1572</u></b> Protocol Tunneling	<b><u>T1573.002</u></b> Asymmetric Cryptography

## 🔪 Indicators of Compromise (IOCs)

TYPE	VALUE
<b>IPv4</b>	144.202.2[.]71, 207.246.105[.]240, 45.77.121[.]232, 47.90.240[.]218, 45.90.123[.]194, 154.6.91[.]26, 154.6.93[.]22, 154.6.93[.]15,

TYPE	VALUE
IPv4	154.6.93[.]12, 154.6.93[.]32, 154.6.93[.]24, 184.170.241[.]27, 191.96.106[.]40, 102.129.145[.]232
SHA256	79a9136eedbf8288ad7357dda3a3cd1a57b7c6f82adffd5a9540e16 23bfb63, 6dcc7b5e913154abac69687fcfb6a58ac66ec9b8cc7de7afd8832a906 6b7bdde, 47dacb8f0b157355a4fd59ccbac1c59b8268fe84f3b8a462378b06433 3920622, 334c2d0af191ed96b15095a4a098c400f2c0ce6b9c66d1800f6b74554 d59ff4b
SHA1	e1c6f76085234554e9a47b61105cd45981eb35d2, bbda2ad0634aa535b9df40dc39a2d4dfdd763476

## Patch Links

<https://www.manageengine.com/security/advisory/CVE/cve-2022-47966.html>

<https://fortiguard.com/psirt/FG-IR-22-398>

## References

[https://www.cisa.gov/sites/default/files/2023-09/aa23-250a-apt-actors-exploit-cve-2022-47966-and-cve-2022-42475\\_0.pdf](https://www.cisa.gov/sites/default/files/2023-09/aa23-250a-apt-actors-exploit-cve-2022-47966-and-cve-2022-42475_0.pdf)

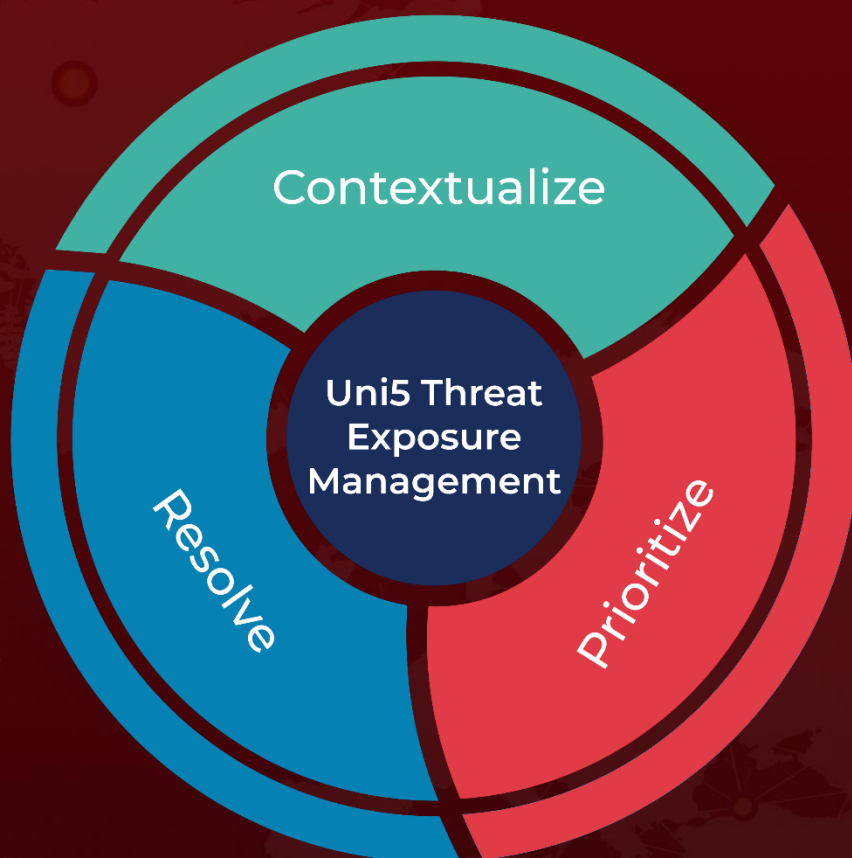
<https://www.hivepro.com/active-exploitation-of-the-fortinet-pre-auth-rce-vulnerability/>

<https://www.hivepro.com/cisas-known-exploited-vulnerability-catalog-january-2023/>

# 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

**September 8, 2023 • 7:00 AM**

© 2023 All Rights are Reserved by Hive Pro®



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