Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Fortinet Releases Patch for Pre-announced Critical Vulnerability

Date of Publication	Admiralty Code	TA Number
June 13, 2023	A3	TA2023259

Summary

First Seen: June 9, 2023
Affected Product: FortiOS and FortiProxy SSL-VPN
Impact: Fortinet has addressed a critical vulnerability in FortiOS and FortiProxy SSL-VPN, resolving a heap-based buffer overflow pre-authentication flaw. This update is crucial because the vulnerability enables remote attackers to execute arbitrary code.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-27997	Fortinet heap-based buffer overflow Pre-Auth Vulnerability	FortiOS and FortiProxy SSL-VPN	✓	✓	✓

Vulnerability Details

#1

Fortinet has issued patches to rectify a critical security flaw found in its FortiOS and FortiProxy SSL-VPN, which have the potential to be exploited by malicious actors for achieving remote code execution. CVE-2023-27997 flaw is a significant heap-based buffer overflow Pre-Auth vulnerability in FortiOS and FortiProxy SSL-VPN. Fortinet devices are highly popular firewall and VPN solutions in the market, which also makes them attractive targets for attacks.

#2

It's alarming to note that there are over 250,000 Fortigate firewalls accessible via the Internet, rendering them vulnerable to potential exploitation through a particular bug. Although no direct correlation was established between the recently exposed Volt Typhoon assaults, which specifically targeted vital infrastructure institutions throughout the United States, there remains a potential for the Chinese cyber espionage faction to exploit the CVE-2023-27997 vulnerability. This possibility could enable threat actors to persistently capitalize on unaddressed weaknesses present in widely used software and devices.

#3

This bug has the potential to impact all previous versions of Fortinet devices. Fortunately, the vulnerability has already been resolved in the latest versions of FortiOS-6K7K, FortiProxy, and FortiOS. Interestingly, even version 6.0.17 appears to have received a **fix**, despite the official support for the **6.0 branch** being discontinued last year.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-27997	FortiOS-6K7K : 7.0.5, 7.0.10, 6.4.8, 6.4.6, 6.4.2, 6.4.12, 6.4.10, 6.2.9, 6.2.7, 6.2.6, 6.2.4, 6.2.13, 6.2.12, 6.2.11, 6.2.10, 6.0.16, 6.0.15, 6.0.14, 6.0.13, 6.0.12, 6.0.10, FortiProxy : 7.2.3, 7.2.2, 7.2.1, 7.2.0, 7.0.9, 7.0.8, 7.0.7, 7.0.6, 7.0.5, 7.0.4, 7.0.3, 7.0.2, 7.0.1, 7.0.0, 2.0.9, 2.0.8, 2.0.7, 2.0.6, 2.0.5, 2.0.4, 2.0.3, 2.0.2, 2.0.12, 2.0.11, 2.0.10, 2.0.1, 2.0.0, 1.2.9, 1.2.8, 1.2.7, 1.2.6, 1.2.5, 1.2.4, 1.2.3, 1.2.2, 1.2.13, 1.2.12, 1.2.11, 1.2.10, 1.2.1, 1.2.0, 1.1.6, 1.1.5, 1.1.4, 1.1.3, 1.1.2, 1.1.1, 1.1.0 and FortiOS : 7.2.4, 7.2.3, 7.2.2, 7.2.1, 7.2.0, 7.0.9, 7.0.8, 7.0.7, 7.0.6, 7.0.5, 7.0.4, 7.0.3, 7.0.2, 7.0.11, 7.0.10, 7.0.1, 7.0.0, 6.4.9, 6.4.8, 6.4.7, 6.4.6, 6.4.5, 6.4.4, 6.4.3, 6.4.2, 6.4.12, 6.4.11, 6.4.10, 6.4.1, 6.4.0, 6.0.9, 6.0.8, 6.0.7, 6.0.6, 6.0.5, 6.0.4, 6.0.3, 6.0.2, 6.0.16, 6.0.15, 6.0.14, 6.0.13, 6.0.12, 6.0.11, 6.0.10, 6.0.1, 6.0.0	cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:* cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*:*:*:*	CWE-122

Recommendations

Comprehensive security Enhancement Measures: To bolster your cybersecurity defenses, it is strongly advised to maintain good cyber hygiene by promptly following vendor **patching** recommendations, adhering to hardening guidelines like the **FortiOS 7.2.0 Hardening Guide**, and minimizing the attack surface by disabling unused features and managing devices through an out-of-band method whenever possible. Implement robust network monitoring tools to detect any suspicious or anomalous activity. This can help identify potential attacks or exploitation attempts and allow for timely response and mitigation.

Safeguarding Against Potential Exploitation: Administrators are strongly advised to take immediate action and update their Fortinet devices as a crucial step in mitigating the risks linked to this vulnerability. Neglecting to address this issue significantly raises the probability of potential exploitation by malicious actors in the near future. Fortinet has consistently demonstrated a proactive approach by releasing security patches prior to disclosing critical vulnerabilities, allowing sufficient time for device updates to prevent threat actors from reverse-engineering the patches. It is worth noting that malicious entities frequently attempt to scrutinize disparities between older and newer operating system versions to discern the patch's intent and exploit any remaining vulnerabilities.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0003** Persistence	**TA0004** Privilege Escalation	**TA0005** Defense Evasion
TA0040 Impact	**T1203** Exploitation for Client Execution	**T1059** Command and Scripting Interpreter	**T1190** Exploit Public-Facing Application
T1588 Obtain Capabilities	**T1588.006** Vulnerabilities	**T1588.005** Exploits	

Patch Details

To address the identified vulnerability, it is essential to upgrade to the following patch versions: FortiOS version 7.4.0,7.2.5,7.0.12,6.4.13,6.2.14,6.0.17 or above FortiProxy version 7.2.4,7.0.10,2.0.13 or above FortiOS-6K7K version 6.4.13,6.2.15,6.0.17 or above

Patch Link:
https://www.fortiguard.com/psirt/FG-IR-23-097

References

https://www.fortiguard.com/psirt?date=06-2023&severity=5

https://www.fortinet.com/blog/psirt-blogs/analysis-of-cve-2023-27997-and-clarifications-on-volt-typhoon-campaign

https://www.helpnetsecurity.com/2023/06/11/cve-2023-27997/

https://www.bleepingcomputer.com/news/security/fortinet-fixes-critical-rce-flaw-in-fortigate-ssl-vpn-devices-patch-now/

https://www.securityweek.com/fortinet-patches-critical-fortigate-ssl-vpn-vulnerability/

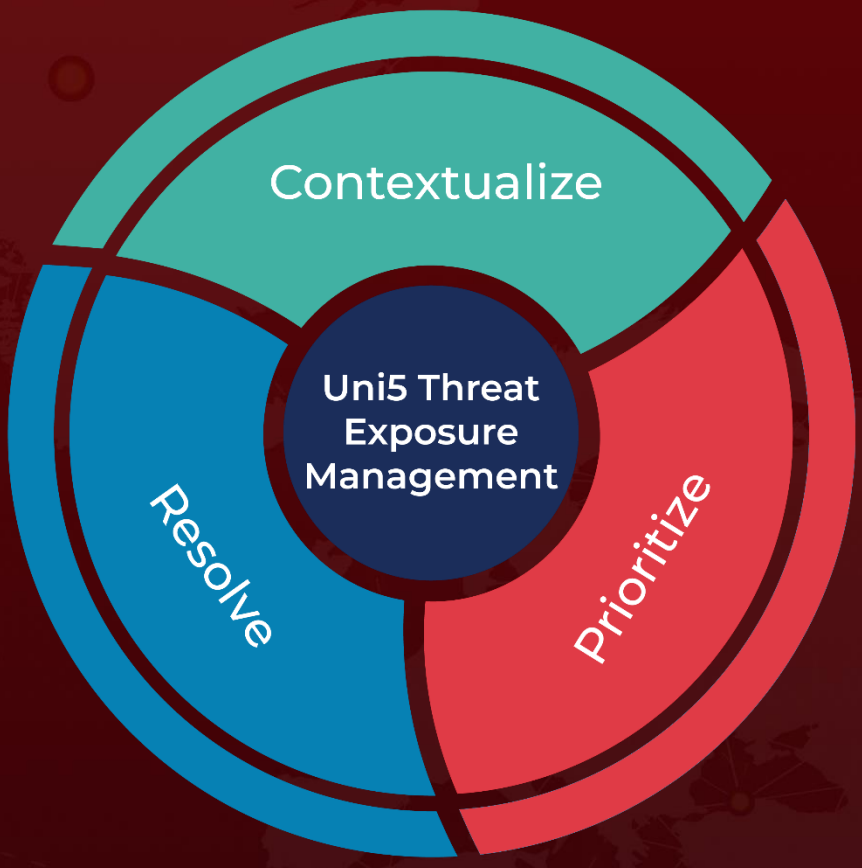
https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/critical-severity-vulnerability-fortinet-fortigate-ssl-vpn-devices

https://www.hivepro.com/volt-typhoon-chinese-espionage-group-targets-u-s-government/

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

June 13, 2023 • 12:23 AM

More at www.hivepro.com