Analysis of CVE-2023-27997 and Clarifications on Volt Typhoon Campaign | Fortinet Blog

By Carl Windsor

Published: 2023-06-12 · Archived: 2026-04-05 15:10:18 UTC

Affected Platforms: FortiOS
Impacted Users: Targeted at government, manufacturing, and critical infrastructure
Impact: Data loss and OS and file corruption
Severity Level: Critical

Today, Fortinet published a CVSS Critical PSIRT Advisory (FG-IR-23-097 / CVE-2023-27997) along with several other SSL-VPN related fixes. This blog adds context to that advisory, providing our customers with additional details to help them make informed, risk-based decisions, and provides our perspective relative to recent events involving malicious actor activity.

The following write-up details our initial investigation into the incident that led to the discovery of this vulnerability and additional IoCs identified during our ongoing analysis.

Incident Analysis

Following previous incident FG-IR-22-398 / CVE-2022-42475 published on January 11, 2023—where a heap-based buffer overflow in FortiOS SSL VPN with exploitation was observed in the wild—the Fortinet Product Security Incident Response Team (PSIRT) proactively initiated a code audit of the SSL-VPN module as part of our commitment to product security and integrity. This audit, together with a responsible disclosure from a third-party researcher, led to the identification of certain issues that have been remediated in the current firmware releases.

Incident ID	NVD CVE	Product	Severity	Description
FG-IR-23-097	CVE-2023-27997	FortiOS	9.2 (Critical)	Heap buffer overflow in SSL-VPN pre-authentication
FG-IR-23-111	CVE-2023-29180	FortiOS	7.3 (High)	Null pointer de-reference in SSLVPNd

FG-IR-22-475	CVE-2023-22640	FortiOS	7.1 (High)	FortiOS - Out-of-bound-write in SSLVPNd
FG-IR-23-119	CVE-2023-29181	FortiOS	8.3 (High)	Format String Bug in Fclicense daemon
FG-IR-23-125	CVE-2023-29179	FortiOS	6.4 (Medium)	Null pointer de-reference in SSLVPNd proxy endpoint
FG-IR-22-479	CVE-2023-22641	FortiOS	4.1 (Medium)	Open redirect in SSLVPNd

Our investigation found that one issue (FG-IR-23-097) may have been exploited in a limited number of cases and we are working closely with customers to monitor the situation.

For this reason, if the customer has SSL-VPN enabled, Fortinet is advising customers to take immediate action to upgrade to the most recent firmware release. If the customer is not operating SSL-VPN the risk of this issue is mitigated – however, Fortinet still recommends upgrading.

Clarifications on Volt Typhoon Campaign

Our own research, conducted in collaboration with our customers, has identified that the Volt Typhoon campaign uses a variety of tactics, techniques, and procedures (TTPs) to gain access to networks, including a widely used technique known as “living off the land” to evade detection. The campaign appears to use vulnerabilities for which patches exist, primarily FG-IR-22-377 / CVE-2022-40684 for initial access, as Indicators of Compromise – admin accounts name `fortinet-tech-support` and `fortigate-tech-support` were found in customer devices related to this campaign.

At this time we are not linking FG-IR-23-097 to the Volt Typhoon campaign, however Fortinet expects all threat actors, including those behind the Volt Typhoon campaign, to continue to exploit unpatched vulnerabilities in widely used software and devices. For this reason, Fortinet urges immediate and ongoing mitigation through an aggressive patching campaign.

Recommended Actions

In addition to monitoring Security Advisories and the immediate patching of systems, Fortinet strongly recommends the following:

- Review your systems for evidence of exploit of previous vulnerabilities e.g. FG-IR-22-377 / CVE-2022-40684

- Maintain good cyber hygiene and follow vendor patching recommendations
- Follow hardening recommendations, e.g., FortiOS 7.2.0 Hardening Guide
- Minimize the attack surface by disabling unused features and managing devices via an out-of-band method wherever possible

Additional Guidance

As a forward-looking security vendor, Fortinet's Product Security Team is constantly seeking ways to engage, inform, and encourage our customers to institute mitigation best practices and to patch their systems.

If a customer should need additional guidance, they are advised to reach out to customer support.

Please contact Fortinet Security via the Submission Form if you have any other suggestions or feedback.

Fortinet continues to follow its PSIRT processes and best practices to best mitigate the situation.

For details of the Fortinet PSIRT Policy: https://www.fortiguard.com/psirt_policy.
