VULNERABILITY BULLETINS

Update: Fortinet FortiGate SSL VPN Critical Remote Code Execution (RCE) Flaw

TLP:WHITE

Jun 13, 2023

Updated Alert:

On June 12, Fortinet issued a PSIRT advisory and a blog post on a critical heap-based buffer overflow vulnerability in SSL-VPN pre-authentication, that was speculated to be a trigger for the latest security updates. The vulnerability tracked as CVE-2023-27997, permits unauthenticated remote code execution (RCE) on the compromised machine. The flaw was discovered through a proactive code review of the SSL-VPN module.

According to Fortinet's blog post, the investigation discovered that the vulnerability was potentially exploited on multiple occasions in attacks targeting government, manufacturing and critical infrastructure organizations. Vulnerabilities that allow authentication bypass are a common target for threat actors that utilize them as an entry point, therefore caution is advised. In prior exploitation cases, Fortinet recognized admin accounts with the names 'fortinet-tech-support' and 'fortigate-tech-support' as indicators of compromise (IoCs) on infected devices, and they may be worth monitoring in this case as well.

Other vulnerabilities that were covered with the latest security updates were:

- *CVE-2023-29180 - Null pointer de-reference in SSLVPNd*
- *CVE-2023-22640 - FortiOS - Out-of-bound-write in SSLVPNd*
- *CVE-2023-29181 - Format String Bug in Fclicense daemon*
- *CVE-2023-29179 - Null pointer de-reference in SSLVPNd proxy endpoint*
- *CVE-2023-22641 - Open redirect in SSLVPNd*

Fortinet recommends:

- *Immediate patching of systems*
- *Review your systems for evidence of exploit of previous vulnerabilities e.g. (IOCs -`fortinet-tech-support` and `fortigate-tech-support`)*
- *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*

Fortinet, a cybersecurity business and VPN service provider, provided security patches on June 9, 2023, which are thought to be a fix for a recently found, significant pre-authentication remote code execution vulnerability in secure socket layer (SSL) VPN devices. The details of the vulnerability have currently been hidden, presumably to allow customers to patch the flaw before it could be exploited.

This vulnerability, tracked as CVE-2023-27997, allows an attacker to run unauthorized code or commands remotely on the compromised system. Researchers claim threat actors could tamper with the VPN even if multifactor authentication (MFA) was used.

Analysis:

CVE-2023-27997 is a critical remote code execution vulnerability that can be exploited by an attacker to execute arbitrary code on a vulnerable device. The vulnerability is pre-authenticated, which indicates that it can be exploited without the need for valid credentials. The previously identified vulnerability is particularly dangerous and should be patched immediately as threat actors may employ reverse engineering techniques to uncover and exploit the vulnerability. There is no evidence the vulnerability has been exploited so far.

Furthermore, per Shodan search, over 250,000 Fortigate firewalls can be accessed from the internet and affects all previous versions, which are more than likely exposed. In the past, SSL-VPN flaws have been exploited by threat actors just days after patches become available and used to gain initial access to networks to conduct data theft and ransomware attacks. Health-ISAC's Threat Operation Center will send out targeted alerts to member institutions that may be impacted.

Fortinet has yet to publish its own advisory on its PSIRT advisory website; however, more details on the vulnerability are expected on June 13, 2023. Health-ISAC will continue to monitor the vulnerability and provide pertinent updates as they are made available.

Security updates addressing the vulnerability are available for active FortiOS firmware versions 6.2.15, 6.4.13, 7.0.12, 7.2.5, and 6.0.17 which is no longer supported.

Recommendations:

Fortinet has released a security patch to address the vulnerability. It is highly recommended that all users of affected FortiGate SSL VPN devices immediately apply the security update. The patch can be

obtained from the official Fortinet support website or through Fortinet's authorized channels.

In cases where immediate patching is not possible, Fortinet has provided some mitigation recommendations to reduce the risk of exploitation:

- Restrict external access to the FortiGate SSL VPN devices by allowing connections only from trusted IP addresses or networks.
- Monitor network traffic for any suspicious activity related to the FortiGate devices, especially SSL VPN traffic.
- Deploy additional network security measures, such as intrusion prevention systems (IPS) or next-generation firewalls (NGFW), to detect and block potential attacks targeting the vulnerability.

It is strongly advised to follow the mitigation steps until the security patch can be applied to ensure the security of your FortiGate SSL VPN devices and the protected network.

Reference(s)	Bleeping Computer, Fortiguard, Help Net Security, Fortinet, Fortiguard

Release Date
1686628799

Alert ID 03160176

View Alert

Tags CVE-2023-27997, Fortigate, RCE, SSL

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions and/or Comments

Please email us at contact@h-isac.org

Share Threat Intel

For guidance on sharing indicators with Health-ISAC via CSAP, please visit the Knowledge Base article CSAP “Share Threat Intel” Documentation at the link address provided here: https://health-isac.cyware.com/webapp/user/knowledge-base Additionally, this collaborative medium provides opportunities for attributed or anonymous sharing across ISACs and other cybersecurity-related entities.

Turn off Categories

For guidance on disabling this alert category, please visit the Knowledge Base article CSAP "Alert Categories" Toggle Documentation at the link address provided here: https://health-isac.cyware.com/webapp/user/knowledge-base

Knowledge Base

Check out our Knowledge Base for HITS integration documentation. https://health-isac.cyware.com/webapp/user/knowledge-base/f4b0c136/

Download Health-ISAC’s Information Sharing App.  

For more update and alerts, visit: **https://health-isac.cyware.com**