JO-FinCERT – Security Advisory – 2023 – 43

1. Critical FortiOS and FortiProxy Vulnerability Exploited

This vulnerability has potentially been exploited in attacks affecting government, manufacturing, and critical infrastructure entities. The vulnerability identified as CVE-2023-27997 / FG-IR-23-097, involves a heap-based buffer overflow weakness in FortiOS and FortiProxy SSL-VPN. It enables unauthorized attackers to achieve remote code execution by leveraging specifically crafted requests without authentication.

The discovery of CVE-2023-27997 occurred during a thorough examination of the SSL-VPN module following a previous series of attacks against government organizations that exploited the CVE-2022-42475 FortiOS SSL-VPN zero-day vulnerability.

1. CVE-2023-27997: Heap buffer overflow in SSL-VPN pre-authentication. CVSS of 9.2/Critical.
2. CVE-2022-42475: Allows a remote unauthenticated attacker to execute arbitrary code or commands via specifically crafted requests. CVSS of 9.2/ Critical.

Recommendations:

- Check your systems for evidence of previous vulnerability exploits (e.g., FG-IR-22-377 / CVE-2022-40684).
- Maintain good cyber hygiene and follow vendor patching recommendations.
- Follow hardening guidelines, such as the FortiOS 7.2.0 Hardening Guide.
- Minimize the attack surface by disabling unused features and using out-of-band management whenever possible.

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

2. Cybercriminals Are Using Powerful BatCloak Engine to Make Malware Fully Undetectable

BatCloak, a malware obfuscation engine, is being utilized to deploy different types of malware with complete stealth, making them fully undetectable (FUD) by antivirus software.

This obfuscation engine enables threat actors to effortlessly load multiple malware families and exploits through batch files that are highly obfuscated. In fact, out of the 784 artifacts examined, approximately 79.6% of them remain undetected by all security solutions. This emphasizes the effectiveness of BatCloak in evading traditional detection methods commonly employed by antivirus systems.

Reference: https://thehackernews.com/2023/06/cybercriminals-using-powerful-batcloak.html