CVE - 2023 - 27997

De Silva K.R.K.D

2023/11/02

INTRODUCTION

A serious heap buffer overflow vulnerability known as CVE-2023-27997 affects the SSL-VPN pre-authentication module of Fortinet's FortiOS. Because of this vulnerability, data from an allocated memory block may overflow into neighboring memory blocks in the execution of arbitrary code and allow for malicious program behavior. Even with Multi-Factor Authentication turned on, a serious flaw in FortiGate SSL VPN could let hackers gain access to weak systems and insert malicious code. [1]

800 requests will be sent to the vulnerable URL path by tool. This results in a measurable timing difference(about 250 microseconds on our devices during testing) between requests with valid and invalid lengths, which we can detect using some math. Half of the requests will therefore be rejected by newer versions of FortiGate. Request size and data length fields are deliberately selected so that memory corruption on susceptible devices affects only the parts of the heap where no data is used. This ensures that there won't be a crash in the SSL VPN process. [2]

A heap-based buffer overflow vulnerability exists in the following versions of FortiOS 7.2.4 and below; 7.0.11 and below; and in the following versions of FortiProxy; 7.2.3 and below; 7.0.9 and below; 2.0.12 and below; 1.2 all versions; 1.1 versions. With carefully constructed requests, an SSL-VPN may enable a remote attacker to run any code or commands. [3]

Table Of Content

Heap Overflow Attack

A heap overflow is a type of buffer overflow that affects the heap, the dynamically allocated memory area. It is also referred to as a heap overrun or heap smashing. Heap overflows, in contrast to stack-based overflows, aim to access memory that is allocated at runtime and typically holds the program data. Attackers take advantage of this vulnerability by modifying data in particular ways and tampering with internal structures, such as pointers to linked lists. The usual technique modifies program function pointer by overwriting dynamic memory allocation data, such as malloc metadata, which could result in arbitrary code execution and unauthorized access. In order to avoid exploitation, heap risks and need to be carefully mitigated.

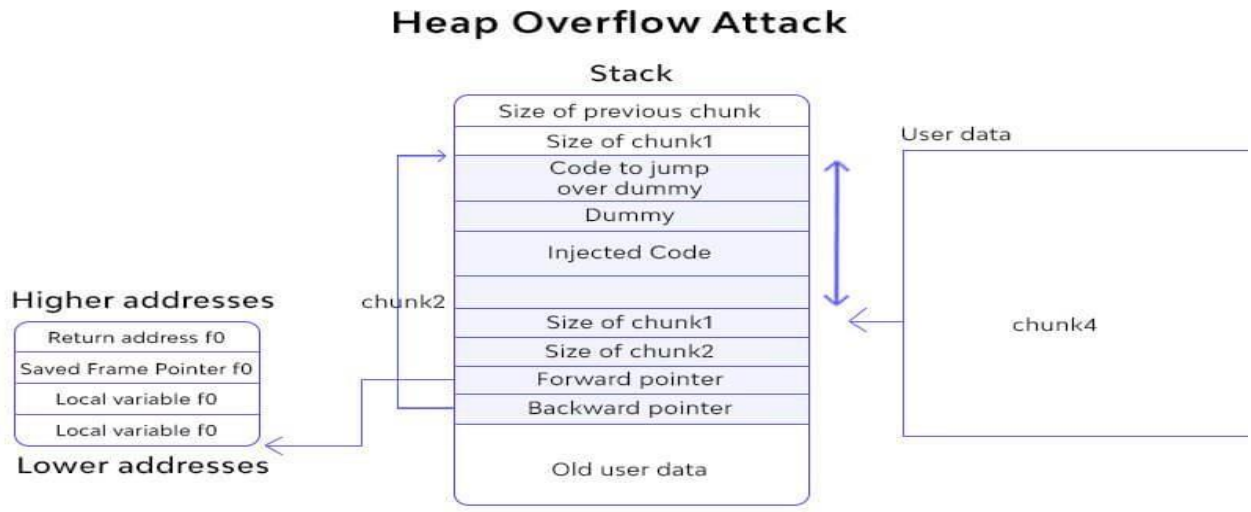
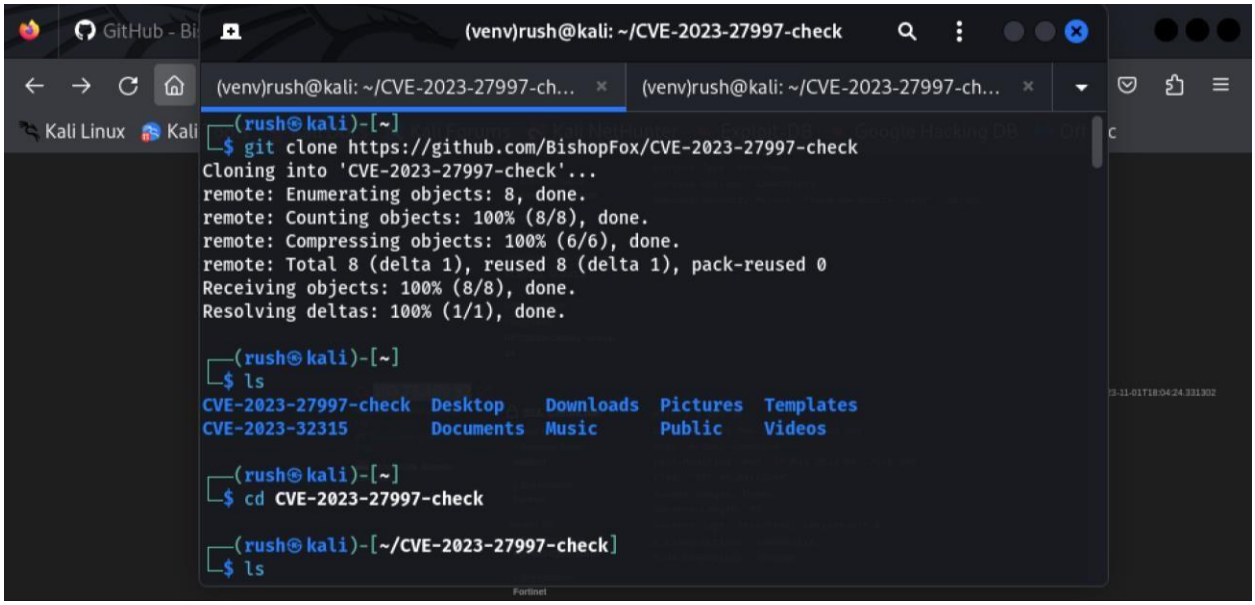


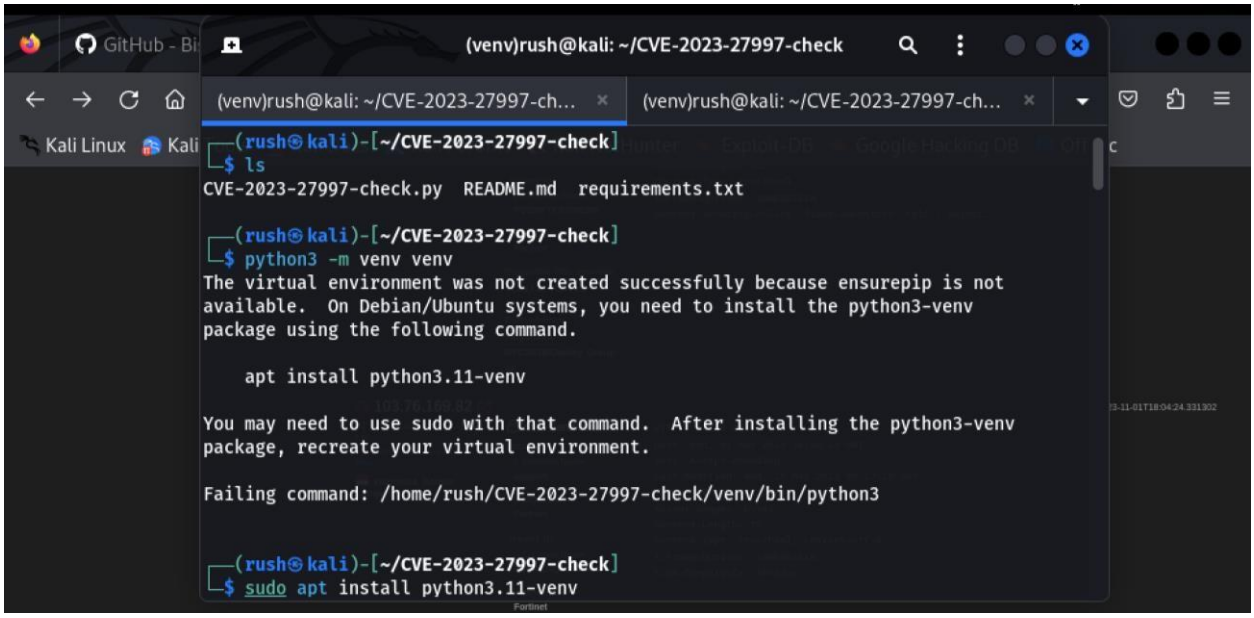
Figure1: Heap Overflow Attack workflow -Wallarm.com

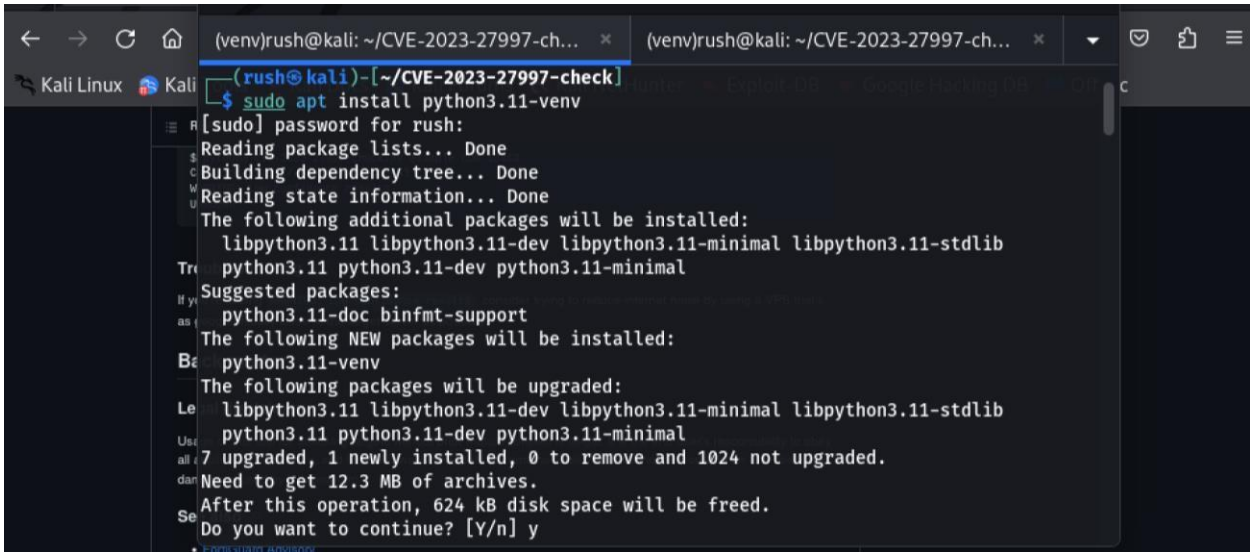
Steps of Exploitation

I used to exploit this vulnerability to some IP addresses and GitHub cloning. First, I cloned my local machine to this GitHub repository https://github.com/BishopFox/CVE-2023-27997-check. If it was successfully cloned I changed its directory to “CVE-2023-27997-check”

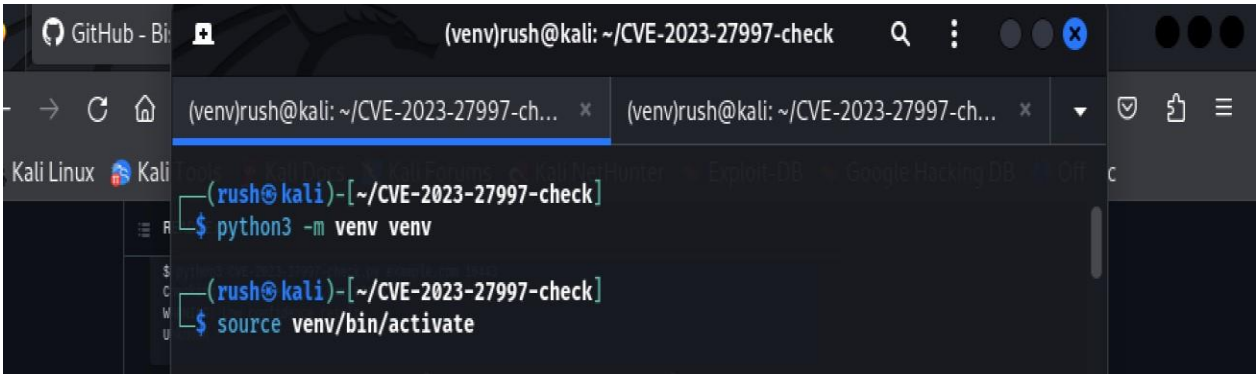


After that I used “python3-m venv venv” command to create a python virtual environment of CVE-2023-27997”. But it didn’t work that time. Because I didn’t install python 3.11. I used to install it to “sudo apt install python3.11-venv”. So this command is used to install the python3.11-venv package on a Linux distribution.

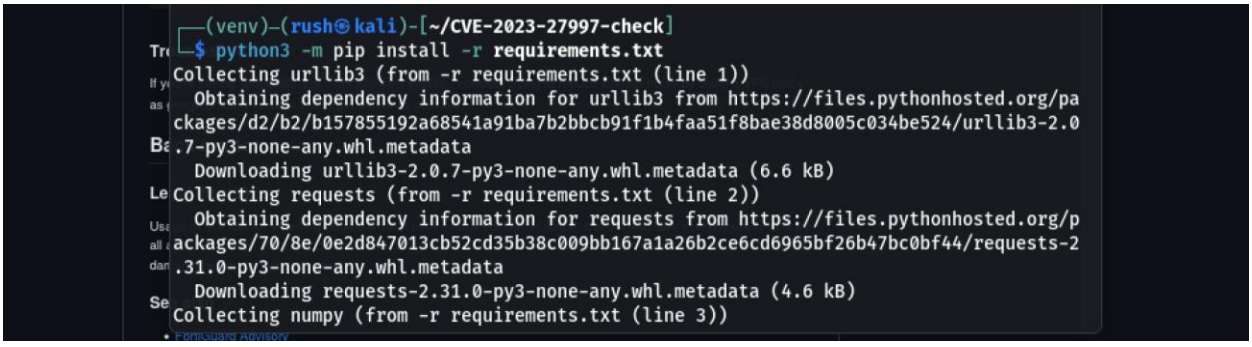




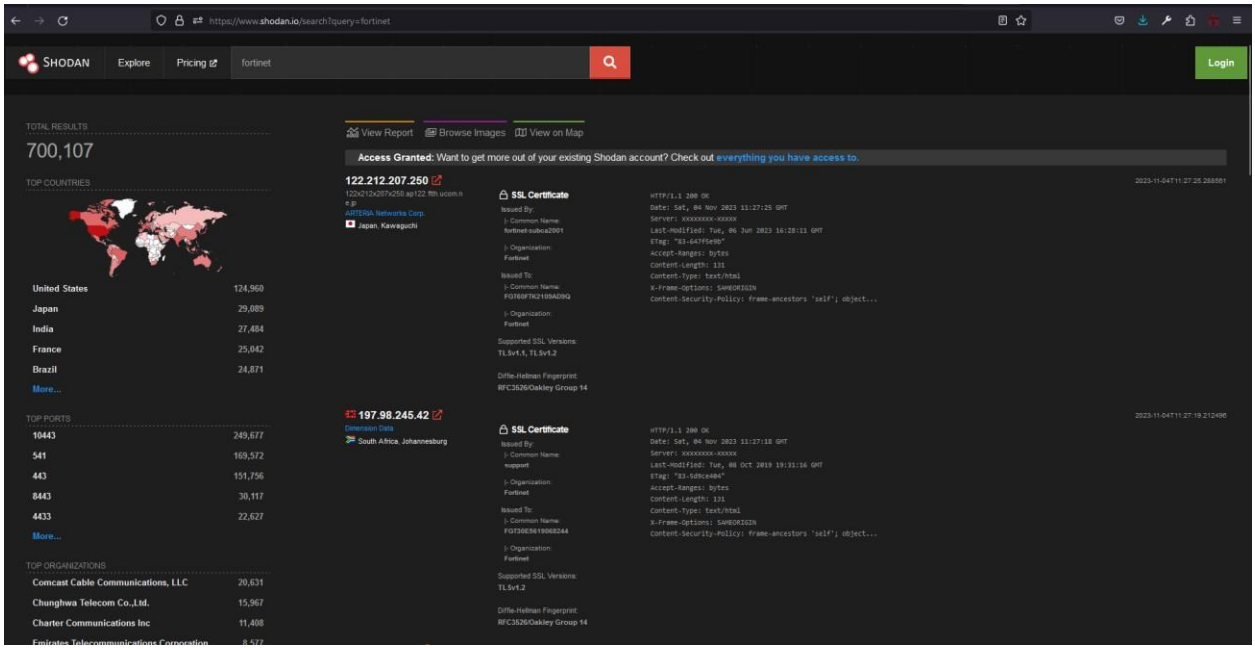
After that again I used that “python3-m venv venv” command. And this command “source venv/bin/activate” to activate a Python virtual environment.



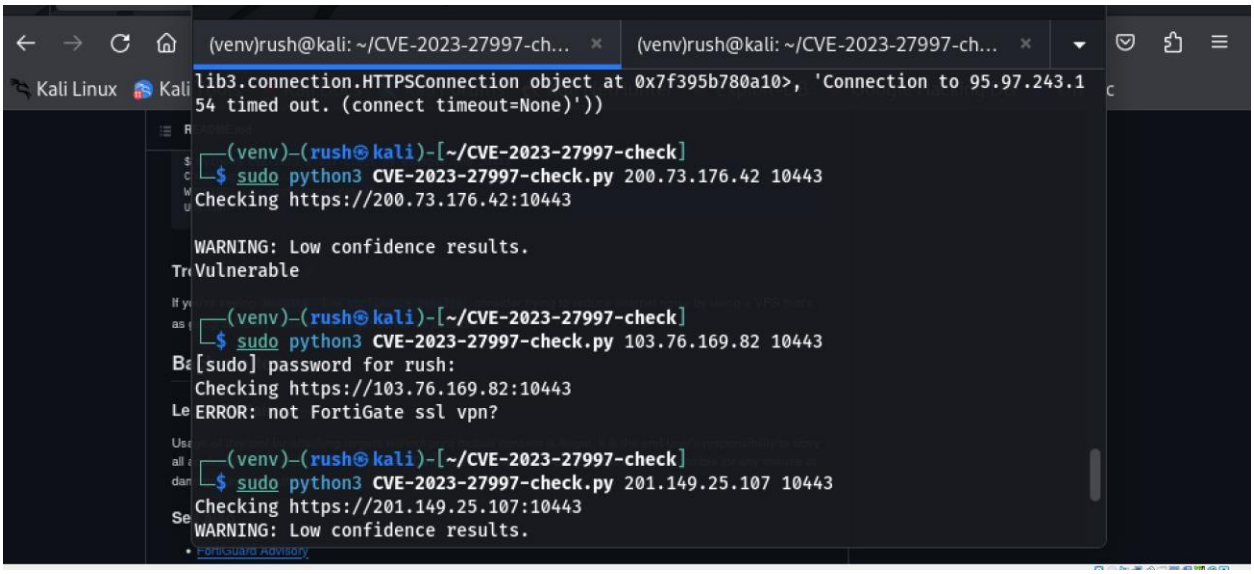
This GitHub repository gives the required text file and I installed it to continue this exploitation.

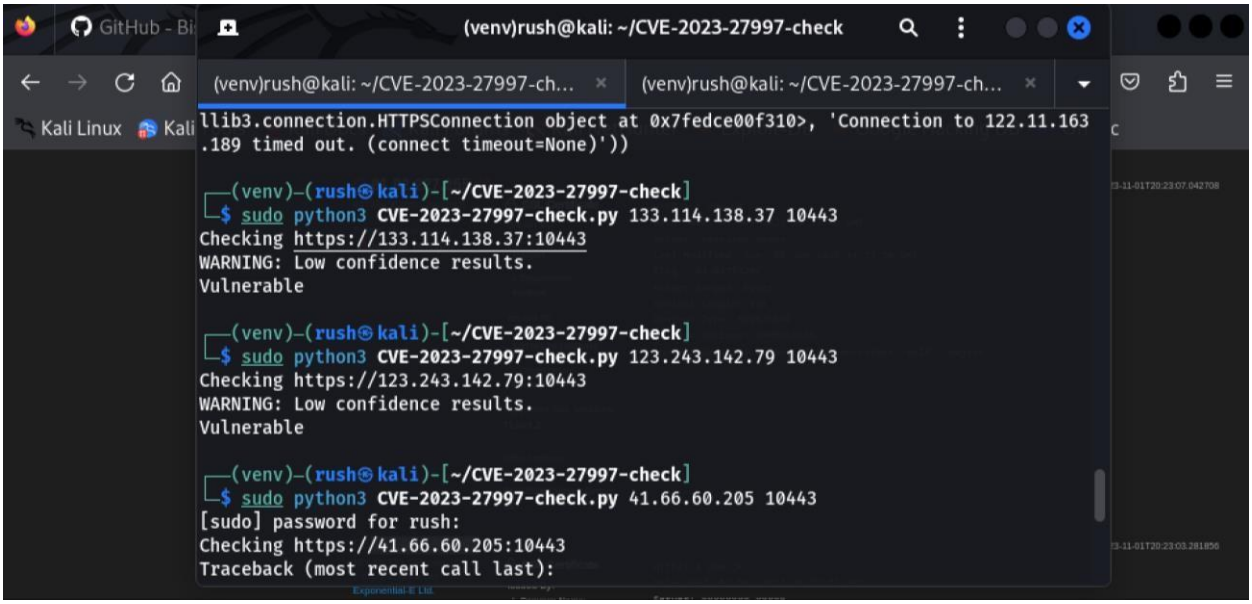


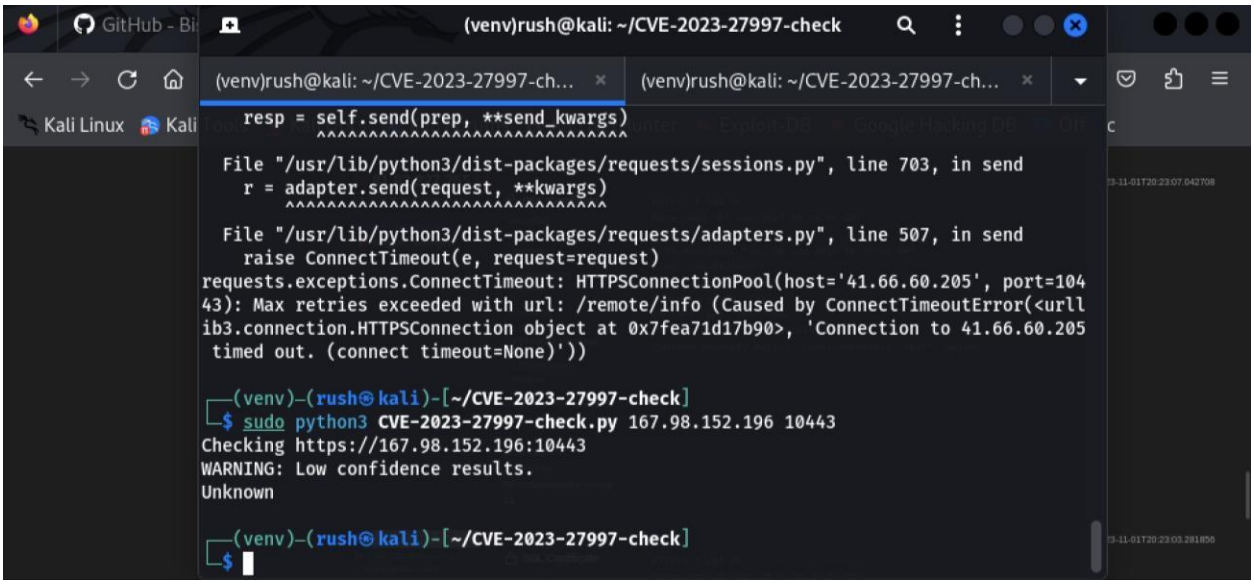
So then, I brows to shodan.io website and search “Fortinet” to find some target Ip addresses.



After all, I used some IP addresses to exploit this vulnerability.







Some results were wrong and the tool warned to me. And some IP addresses were vulnerable.

How to Detect

- Upgrade to the latest FortiOS Firmware Release
- Disable SSL-VPN on all impact devices
- Follow FortiOS guidelines

CONCLUSION

In conclusion, a server heap buffer overflow vulnerability, identified as CVE-2023-27997, has been discovered in Fortinet's FortiOS SSL-VPN preauthentication module. This vulnerability permits data overflow from an allocated memory block into adjacent memory regions, potentially allowing for the execution of malicious code and unauthorized program behavior. Even with multifactor authentication enabled, a significant flaw in FortiGate SSL VPN exposes the risk of hackers gaining access to vulnerable systems and inserting malicious code. Several versions of FortiOS and FortiProxy are vulnerable to this heap-based buffer overflow vulnerability, which could allow a remote attacker to run any code or commands with skillfully constructed requests. In order to mitigate this security risk and safeguard susceptible systems, prompt attention and action are needed.

References

[1] E. Kost, "UpGuard (How To Respond: CVE-2023-27997)(Fortigate SSL VPN)," 01 August 2023. [Online]. Available: https://www.upguard.com/blog/how-to-respond-cve-2023-27997#toc-0.

[2] "GitHUb(CVE-2023-27997 Vulnerability Assessment Tool)," [Online]. Available: https://github.com/BishopFox/CVE-2023-27997-check.

[3] "NIST(CVE-2023-27997 Details)," 13 06 2023. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2023-27997.