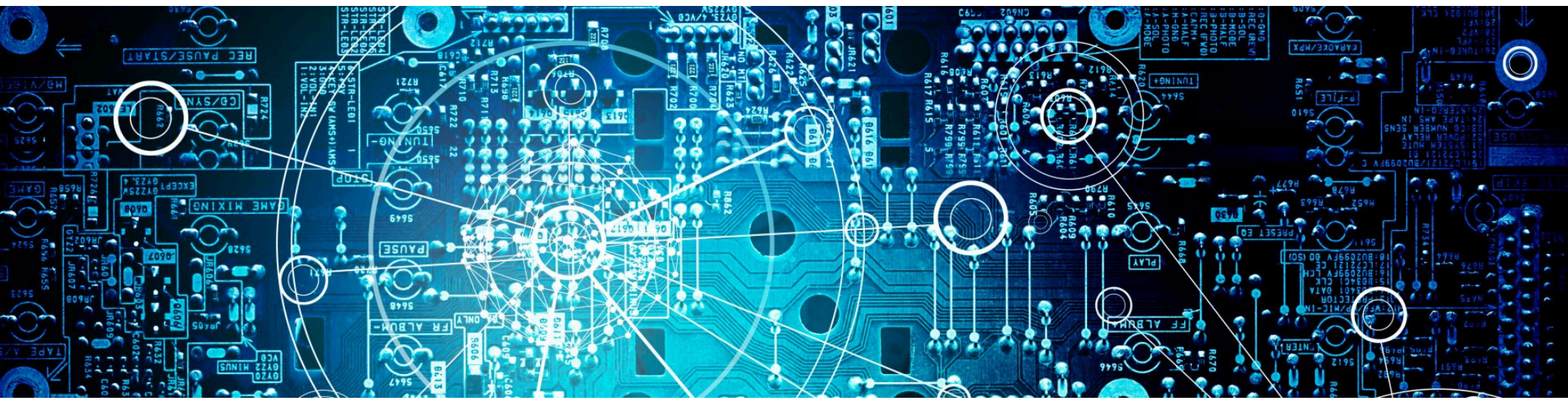

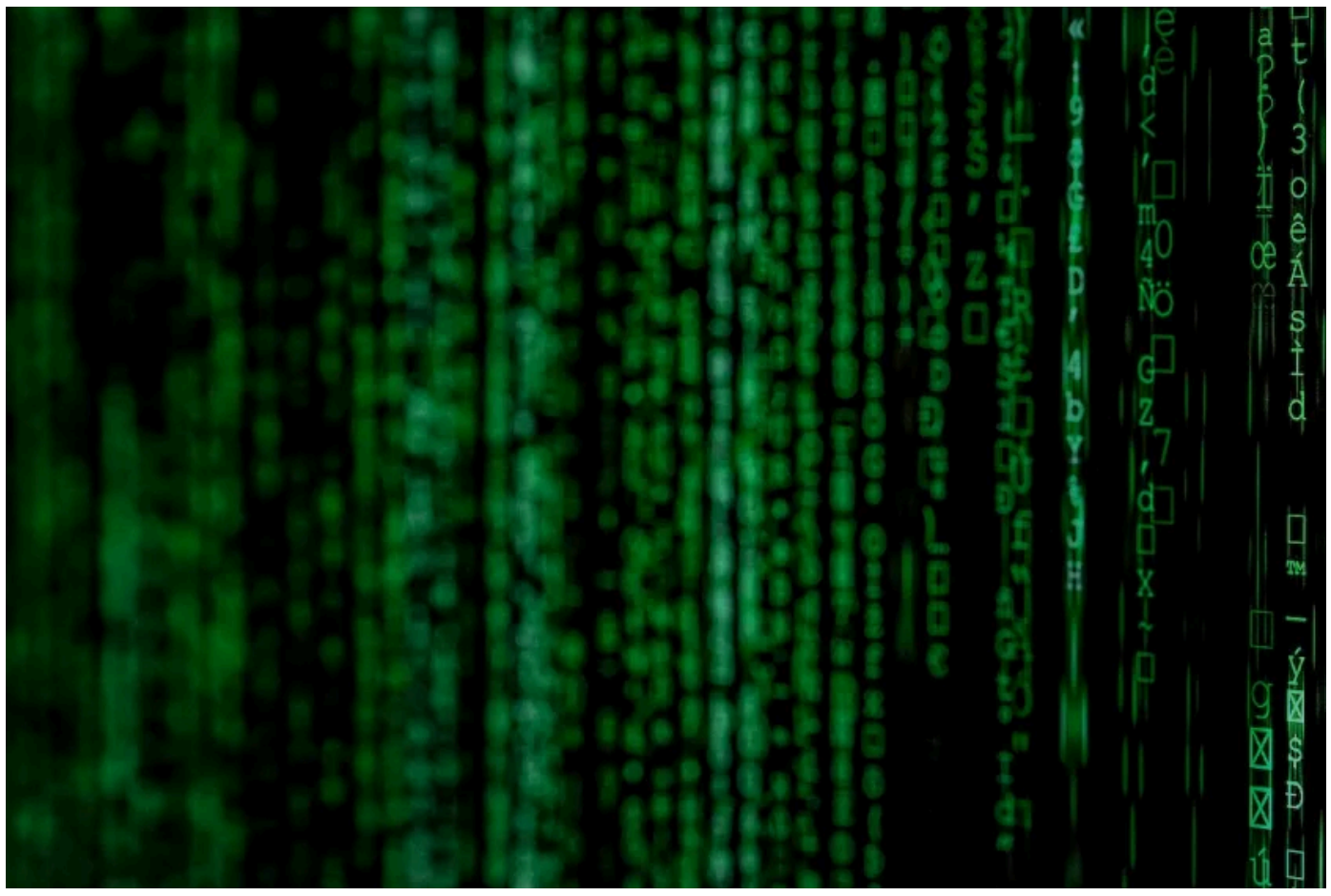

SEARCH

Search …

CATEGORIES

Select Category

ARCHIVES

Select Month

CVE-2023-27997 – PRE-AUTHENTICATION RCE ON FORTIGATE SSL-VPN

June 12, 2023 KS Threat Research Security Advisory Leave a comment

Written by Harish Segar and Scott Emerson of the Kudelski Security Threat Detection & Research Team

---

June 13th, update 2: Technical details of bug and exploitation disclosed at https://blog.lexfo.fr/xortigate-cve-2023-27997.html

---

Summary

TWITTER @KUDELSKISEC

My Tweets

On Friday, June 9th, Fortinet issued firmware updates for Fortigate appliances addressing a possible critical pre-authentication remote code execution (RCE) vulnerability found in SSL VPN.

Unfortunately, that release note did not mention that they included a fix for CVE-2023-27997. Security researchers Charles Fol and Dany Bach of **LEXFO** revealed additional information, stating that the new FortiOS updates include a fix for a critical RCE vulnerability that they discovered.

Technical details on the bug and exploitation process were disclosed Tuesday, June 13th, 2023 by Charles Fol on LEXFO's blog. The CVSS score is a Critical 9.2, "but really, it's a 10," quips the researcher.

Fortinet's appliances are among the most popular firewall and VPN devices on the market, making them a prime target for attacks. An investigation on Shodan uncovered that there are more than 250,000 Fortigate firewalls accessible from the internet. Considering that this vulnerability impacts all previous versions, the majority of those appliances are likely vulnerable. Historical evidence shows that SSL VPN flaws have been exploited by threat actors just days after patches are released.

Due to the potential for exploitation and abuse of this vulnerability, Kudelski Security strongly recommends that organizations validate that they have applied Fortinet's latest patches to properly mitigate this vulnerability as soon as possible. Now that technical details are publicly available, Kudelski Security expects to see exploitation "in the wild" shortly.

Affected Applications

Per Fortinet's advisory, the following are the affected versions of FortiOS and FortiProxy and the relevant fixed versions:

Product	Affected Versions	Fixed Versions
FortiOS-6K7K	7.0.5, 7.0.10	7.0.12 or above
FortiOS-6K7K	6.4.2, 6.4.6, 6.4.8, 6.4.10, 6.4.12	6.4.13 or above
FortiOS-6K7K	6.2.4, 6.2.6 through 6.2.7, 6.2.9 through 6.2.13	6.2.15 or above
FortiOS-6K7K	6.0.10, 6.0.12 through 6.0.16	6.0.17 or above
FortiOS	7.2.0 through 7.2.4	7.2.5 or above
FortiOS	7.0.0 through 7.0.11	7.0.12 or above
FortiOS	6.4.0 through 6.4.12	6.4.13 or above
FortiOS	6.0.0 through 6.0.16	6.0.17 or above
FortiProxy	7.2.0 through 7.2.3	7.2.4 or above

FortiProxy	7.0.0 through 7.0.9	7.0.10 or above
FortiProxy	2.0.0 through 2.0.12	2.0.13 or above
FortiProxy	All versions of 1.1 and 1.2	2.0.13 or above

Technical Details

The bug was examined by security researchers from **watchTowr**. They performed a "patch diff" to scrutinize the vulnerable and patched software versions at the assembly level.

According to researchers, this is a heap overflow bug, but more precisely the problem originates from the truncation of a payload length to 8 bits, followed by an insufficient length check. As a result, an attacker can create an **encData** value with a payload length that surpasses the adjusted length check. This can result in out-of-bounds access and unpredictable behavior. For further detail, the full watchTowr blogpost can be found here.

WatchTowr's findings on CVE-2023-27997 were later confirmed and expanded upon by Charles Fol in a blogpost for LEXFO. In addition to insight on the bug itself, he walks through the exploitation process on ARM and x64 architectures and shows successful unauthenticated RCE for both on video, though no proof-of-concept code is provided and much is left as an exercise to the reader.

Solution

- Kudelski Security recommends identifying, validating, and implementing a security update for any affected systems as soon as possible. Administrators should move fast and implement the patch as soon as possible. If the update isn't available in the device's dashboard, rebooting the appliance it may make it available. If not, manual download and installation is advised.

- Fortigate users can check if their devices are vulnerable by using the following command on the CLI and comparing with the version table above:

diagnose sys fortiguard-service status

- Users can also use external tools such as Nmap or Shodan to scan their devices for open ports related to SSL VPN (such as 443 or 10443) and check the banner information for the FortiOS version number.

- For clients using Nessus/Tenable, the plugin ID 177116 can be used to identify whether a system is patched for CVE-2023-27997. In addition, plugin ID 73522 can be used to identify Fortinet devices in your network.

Temporary workarounds and mitigations

Disabling SSL-VPN functionality could mitigate the issue, but upgrading your appliances still remains the most effective and recommended solution.

Detection Guidance

According to the LEXFO blogpost, the bug is exploitable by issuing several HTTP GET or POST requests to either or both of the /remote/hostcheck_validate and /remote/logincheck URLs. Simple exploits will make these requests in quick succession, but it is reportedly possible to make them more slowly with careful heap management. Additionally, exploits of poor quality might cause a crash of the /bin/sslvpnd process.

What the Cyber Fusion Center (CFC) is doing

The CFC is investigating the possibility of a threat hunt campaign to identify successful exploitation of this vulnerability, using internal queries and methodology resourced from Incident Response engagements where similar activity was observed.

The CFC is also coordinating with our vulnerability scanning partner to deploy plugins capable of identifying unpatched systems and assets vulnerable to CVE-2023-27997. Once available, organizations with the CFC's Vulnerability Scanning service will be able to validate using the results from the scan.

Sources

- https://twitter.com/cfreal_/status/1667852157536616451
- https://olympecyberdefense.fr/1193-2/
- https://www.fortiguard.com/psirt/FG-IR-23-097
- https://www.fortinet.com/blog/psirt-blogs/analysis-of-cve-2023-27997-and-clarifications-on-volt-typhoon-campaign
- https://labs.watchtowr.com/xortigate-or-cve-2023-27997
- https://blog.lexfo.fr/xortigate-cve-2023-27997.html

CYBERSECURITY SECURITY ADVISORY

« Presenting zekrom: a library of arithmetization-oriented constructions for zkSNARK circuits. Part 1: arkworks-rs

Tales From the Incident Response Cliff Face »

LEAVE A REPLY