# AMERICAN INTERNATIONAL UNIVERSITY–BANGLADESH (AIUB)

## FACULTY OF SCIENCE & TECHNOLOGY

## DEPARTMENT OF CSE

# Network Security

**Fall 2024-2025**

**Section: A**

## Final Term Assignment

**Supervised By**

**MD. MANIRUL ISLAM**

**Submitted By**

**MD. Nasif Sadnan Chowdhury**

**ID: 22-46118-1**

**Date of Submission: 20th January 2025**

# Report on Attack on Danish Critical Infrastructure by Russian Hacking group Sandworm

## Attack Summary

In May of 2023, Denmark faced the worst cyberattack on its critical infrastructure. This uses a vulnerability in Zyxel's firewalls, affecting 22 companies within their energy infrastructure. Some of these companies, in which the industrial control systems got compromised, were forced to operate in emergency island mode. April 25, 2023, A dangerous software error (CVE-2023-28771) in Zyxel firewalls, which are frequently used in critical infrastructure, allows malefactors to take control unlawfully without the use of authorized access. SektorCERT is in urgent need of members to hurry up in doing the necessary updates of their firewalls to solve this immediate problem.

So, on the 11th of May 2023, coordinated attacks against 16 Danish energy companies were executed using severe vulnerabilities (CVE-2023-28771) in Zyxel firewalls. They had already crept into the networks of 11 out of the 16 firms, taking control of their firewalls. That was the first wave of the attack.

On May 22-24, 2023, another wave used newly discovered vulnerabilities (CVE-2023-33009 and CVE-2023-33010) to attack more firms, using firewalls to facilitate further DDoS attacks.

## Exploited Vulnerabilities

Attackers were able to successfully cause three dangerous vulnerabilities in Zyxel firewalls. The vulnerabilities in allowing unauthorized access, remote code execution, and control over the compromised systems.

1. **CVE-2023-28771**: This vulnerability was in the Internet Key Exchange (IKE) packet decoder of VPN, which are the Zyxel devices secure communication controls. The attack scenario an adversary could potentially send one packet portrayed as being legitimate to port 500 and thereby take advantage of the way how a router processes the packets. Process: A malicious packet was crafted by the attackers to abuse the IKE decoder. After the corrupted file is received, the inherent security flaw granted the attacker root-level access, and there was no need for any authentication. The attackers are capable of modifying firewall settings, accessing data and planning new cyber-attacks.

   **Process:** The attack involved developing a packet that targeted the IKE decoder. When this packet is received the system allows the execution of code at root level without any form of authentication. Firewalls can be changed to permit further access and infiltration of data and even establish a new fresh ground for the attackers.

   **Impact:** As a consequence of the manageable requirements - simplicity and no special technical nuances, this particular vulnerability appeared to be of medium threat classification, but it actually was extremely serious. It was exploited to gain access to the firewalls of 11 companies in the course of the first wave of attacks on May 11, 2023. The calculated CVSS score of this vulnerability was 9.8 out of 10, which tells about its high severity; the company and the user were notified by Zyxel about this vulnerability on April 25, 2023, whereas unpatched systems were still the problem.

2. **CVE-2023-33009 and CVE-2023-33010**
   The security vulnerabilities occurred in buffer overflow that affects specific functions such as the Zyxel firewall. It can crash the applications either by running them with a payload or with incorrect data.

- **CVE-2023-33009**: Locating in the notification function, it enables attackers to execute remote code or cause denial-of-service (DoS) conditions.

- **CVE-2023-33010**: Again located in the ID processing function and lets attackers either give code execution or crash the device.

**Process:** To this end, during the second wave of attacks (May 22-24, 2023), the attackers exploited these vulnerabilities to gain unauthorised remote control of the firewalls and incorporate them into Distributed Denial of Service (DDoS) botnets. Heavily targeted devices are those which are used against organizations in Canada, Hong Kong, and United States.

**Impact:** Within the CVSS scale, both receive a score of 9.8/10 making the vulnerabilities critically high-risk. Despite the fact that Zyxel published it on May 24, 2023, the attackers utilised the vulnerabilities before this announcement as the zero-day vulnerabilities probably suggest the prior preparation and availability of the resources.

| CVE ID | Vulnerability Type | Attack Process | Impact | CVSS Score | Date published |
|---|---|---|---|---|---|
| CVE-2023-28771 | IKE Decoder Flaw | Malicious packets sent to port 500 exploited the flaw, enabling root access without authentication. | Attackers gained control of firewalls, modified settings, accessed data, and prepared for new attacks. | 9.8/10 | April 25, 2023 |
| CVE-2023-33009 | Buffer Overflow (Notification) | Exploited notification function to cause denial-of-service or remote code execution. | Used in second wave of attacks to integrate compromised systems into DDoS botnets. | 9.8/10 | May 24, 2023 |
| CVE-2023-33010 | Buffer Overflow (ID Processing) | Exploited ID processing function to execute code remotely or crash devices. | Contributed to unauthorized control of firewalls and integration into DDoS botnets. | 9.8/10 | May 24, 2023 |

Table1: Exploited Vulnerabilities and Their Impact

## Remedy Actions Taken

SektorCERT also is ready to assemble teams for responding to attempts from outside and minimize the harm. It also identifies all the affecting companies and tried to addressed the issue by closing down their systems like unplugging them from the outside world. Suppliers try to resolve issues with systems and deploy patches, meanwhile the concerned authorities, such as the National Center for Cybercrime (NC3) and the Center for Cyber Security were informed and involved in the process.

The team for example provides real-time monitoring which helps in capturing and preventing any such access attempts in addition to escalating security measures. Such monitoring is considered important in order to avoid further exploitation. Further, members got awareness through SektorForum concerning new developments and discovery related to the attacks such as what was targeted and what was done and what is to be done in future in case of such attacks.

The team performs real time surveillance to detect and deter such access attempts apart from exercising additional measures. This monitoring is considered important in avoiding more exploitation as seen from the following reasons. Also in this forum SektorForum members received information about the results and findings concerning the attacks, what was hit and done and what could be done in the future in case of similar attacks.

These efforts coupled with the coordination between of SektorCERT, suppliers and all other authorities ensured that the damage resulting from the cyberattacks was limited and the critical infrastructure systems remained optimal without huge interferences.

## Recommended Future Mitigation Strategies

In curbing similar incidences in the future, the following strategies are recommended:

1. **Regular Patching and Updates:** An organisation-wide patch management policy to keep all network and portable devices frequently updated.

2. **Network Segmentation:** The application of network segmentation can be applied in order to restrict the breach scope and secure a portion of infrastructure from the blow an intrusion might cause.

3. **Security Awareness Training:** The IT department should also keep abreast of several such refresher training seminars in due course on timely updates and reiteration of security measures in a professional manner.

4. **Vendor Management:** Service agreements with vendors should specify in detail the kind of updates that will be provided to assure that patching is amongst key service deliverables.

5. **Incident Response Planning:** Maintain crisis management instructions for dealing effectively with a security incident as soon as possible.

## References

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

2. Coker, J. (2023, November 16). *Sandworm Linked to Attack on Danish Critical Infrastructure*. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/russian-sandworm-attack-danish/

3. *Nearly two dozen Danish energy companies hacked through firewall bug in May*. (n.d.). Therecord.media. https://therecord.media/danish-energy-companies-hacked-firewall-bug

4. Jones, C. (n.d.). *How Denmark nulled record attacks on critical infrastructure*. Www.theregister.com. https://www.theregister.com/2023/11/13/inside_denmarks_hell_week_as/

5. Ionut Arghire. (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/