Altergize

Cybersecurity Watch

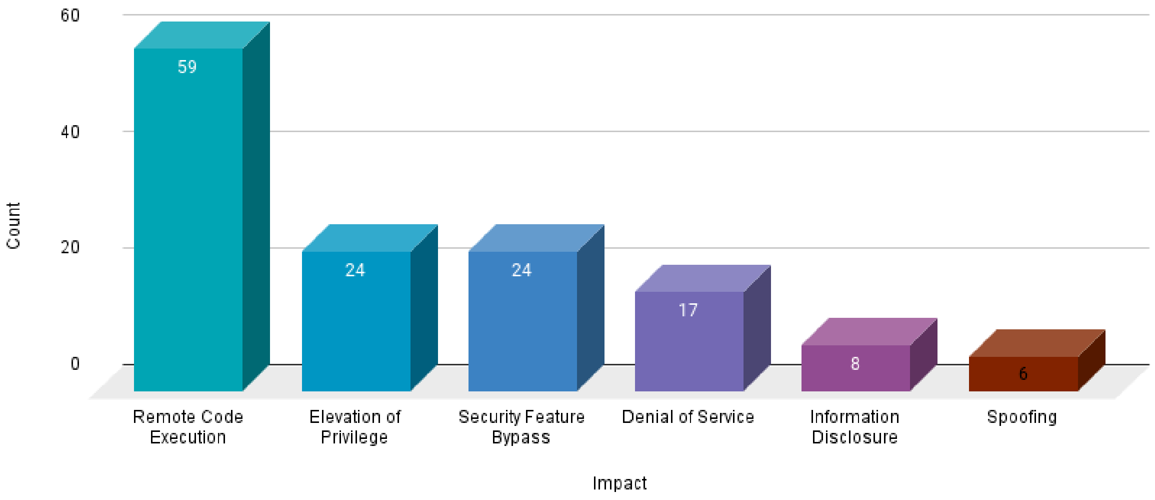
James Pooley
[19/08]

Table of contents

1. Executive Summary

Our analysis has identified several critical vulnerabilities in key software used within our infrastructure, specifically Windows Server, Windows Active Domain Services and MOVEit file transfer. These softwares were chosen for this report because of their critical use in our systems, all operating on varying network ranges.

It is crucial to understand the type of vulnerability, how common they are and how to effectively deal with the vulnerability. Remote Code Execution (RCE) vulnerabilities accounted for 42.8% of the vulnerabilities patched by Microsoft in July, followed by Elevation of Privilege (EoP) and Security Feature Bypass vulnerabilities.



Two critical vulnerabilities to be aware of:

- **Windows - CVE-2024-38063:** An unauthenticated attacker could repeatedly send specially crafted IPv6 packets to a Windows machine which could enable Remote code execution. Does not require any user input for a successful attack.
- **MOVEit - CVE-2024-5806:** Improper Authentication can lead to authentication bypass. Attackers can also exploit this vulnerability to masquerade as any user on the system potentially enabling a data leak.

Both of these vulnerabilities have since been patched by their respective product owners, but we need to ensure that we are regularly updating our software to prevent these vulnerabilities from being exploited by threat actors.

The Network and Information Systems (NIS2) Directive in the EU and the UK's upcoming Cyber Security and Resilience (CSR) Bill both aim to enhance cybersecurity across critical infrastructure, focusing on mandatory incident reporting and expanding the scope of regulated sectors. Similarly, in the U.S., the overhaul of the Federal Information Security Modernization Act (FISMA) strengthens federal cybersecurity measures and inter-agency coordination, while the NIST Cybersecurity Framework 2.0 introduces new standards for governance and supply chain security. Together, these initiatives reflect a global shift toward more rigorous cybersecurity policies to address escalating threats and improve organisational resilience.

Staying informed about recent vulnerabilities and adhering to updated security frameworks is vital for protecting our critical infrastructure. Proactively addressing these issues will improve our security posture, ensuring the reliability and continuity of our energy services while safeguarding sensitive data and maintaining regulatory compliance. This strategic focus on cybersecurity is essential for sustaining all our company's operations and reputation in the renewable energy sector.

2. Identified Technologies

The following software programs were selected for the cybersecurity watch:

Windows server 2019
Active Domain Services
MOVEit file transfer

3. High-Impact Vulnerabilities

Technology	**Vulnerability (CVE-ID)**	**Brief description of the vulnerability**
Windows Server 2019	*CVE-2024-30080*	1. To exploit this vulnerability an attacker would need to send a series of specially crafted (Microsoft Message Queuing) MSMQ packets in rapid sequence over HTTP to a MSMQ server. 2. This could result in remote code execution on the server side.
Windows Server 2019	CVE-2024-38077	1. An authenticated attacker could connect to the Remote Desktop Licensing Service and send a malicious message which could enable remote code execution
MOVEit	CVE-2024-5806	1. Improper Authentication can lead to authentication bypass 2. Attackers can also exploit this vulnerability to masquerade as any user on the system.
MOVEit	CVE-2024-6576	1. Improper authentication vulnerability can lead to Privilege escalation. Used by threat actors to gain unauthorised access due to improper authentication mechanisms
Active Domain Services	CVE-2024-38060	1. An authenticated attacker could exploit the vulnerability by uploading a malicious TIFF file to a server 2. An authenticated attacker could trigger this vulnerability. Does not require admin or elevated privileges.
Active Domain Services	CVE-2024-38063	1. An unauthenticated attacker could repeatedly send specially crafted IPv6 packets to a Windows machine which could enable Remote code execution.

4. Relevant Cyberattacks

Listed below are two critical vulnerabilities that could have a serious impact on Altergize and its normal operations. Both vulnerabilities have now been patched, therefore it is imperative that we ensure all company systems are receiving regular updates to prevent future attacks that could exploit these vulnerabilities.

Attack 1: Windows - CVE-2024-38063
Remote Code Execution (RCE) (CVSS: 9.8)

An unauthenticated attacker could repeatedly send specially crafted IPv6 packets to a Windows machine which could enable RCE. This attack has been rated High for compromising Confidentiality, Availability and Integrity. This vulnerability is particularly concerning because it requires no user interaction for an attack to be successful. Microsoft is not being specific about the root location of the vulnerability but they state that systems are not affected if IPv6 is disabled on the target machine. This vulnerability could impact Altergize but allowing an adversary to access any of our windows systems and deploy malicious code remotely.

Attack 2: MOVEit - CVE-2024-5806
Data Leak (CVSS: 9.1)

On June 25th, software company Progress publicly disclosed a critical severity vulnerability in their managed file transfer software application, MOVEit Transfer. The vulnerability allows a remote attacker to bypass authentication and log in as any valid user on the system. This access could enable the attacker to download files accessible to any user on the MOVEit appliance. Since these appliances are typically used to securely transfer sensitive information, bypassing authentication mechanisms could result in the unauthorised download of a large amount of sensitive data stored on the MOVEit appliance.

5. Security Frameworks and Legislation

Recent updates in cybersecurity regulations in the UK and U.S that focus on improving defence across critical sectors including renewable energy.

Network and Information Systems (NIS) 2 Directive and CyberSecurity and Resilience (CSR) Bill

In the UK, the CSR bill announced in the King's Speech in July 2024 is designed to strengthen the UK's cyber defences to ensure that critical infrastructure and digital services are more secure. This legislation aims to expand upon the existing NIS regulations introduced in 2018. The NIS Regulations initially focused on operators of essential services like energy, health, and digital infrastructure, as well as some digital service providers. However, the CSR Bill will likely broaden its scope to include more sectors and place greater emphasis on the security of supply chains.

The recent update (published in Dec 2022) to the Network and Information Systems (NIS) Directive, known as NIS 2, introduces more stringent security requirements for operators of essential services, including those in the renewable energy sector. It aims to enhance the cybersecurity resilience of critical infrastructure by mandating improved risk management practices, incident reporting protocols, and cooperation among member states. Compliance with NIS 2 is crucial as it emphasises the need for robust cybersecurity frameworks to safeguard against potential disruptions and cyber threats, ensuring the continuity and reliability of energy services.

Federal Information Security Modernization Act (FISMA) Overhaul and National Institute of Standards and Technology (NIST) framework 2.0

Back in 2023 in the United States, FISMA was revamped to improve federal agencies' cyber security postures and foster better coordination across government bodies. This overhaul is significant for managed service providers and contractors working with government agencies because they will need to align their cybersecurity measures with these enhanced standards. The NIST Cybersecurity framework 2.0 released in February 2024, emphasises the governance and supply chain security. This framework is designed primarily for federal agencies and serves as a best practice guide for private sector organisations as well, including small and medium-sized businesses.

The NIS2 Directive and CSR Bill in the UK, along with FISMA and NIST 2.0 in the U.S., all emphasise strengthening cybersecurity across critical sectors. These frameworks focus on enhanced incident reporting, governance, and supply chain security to better protect against evolving cyber threats and improve overall resilience.

6. Sources Used for the Report

Sources

Source #	Title of source	Brief description	Publisher	Link	Justification for including source
1	*Microsoft Patch Tuesday*	*Weekly publication of patches recommended for Microsoft products*	*Microsoft*	*https://msrc.microsoft.com/update-guide/en-us*	*This source is the go-to and most authoritative resource for updates to Microsoft products. It is used as a source of truth by many major organisations.*
2	Authentication Bypass Vulnerability in Progress MOVEit Transfer	A blog detailing the new MOVEit vulnerability and previous MOVEit issues and vulnerabilities	Kroll	https://www.kroll.com/en/insights/publications/cyber/progress-moveit-transfer-cve-2024-5806	Kroll is a financial and risk advisory firm that posts reports on cyber risk and cyber threat intelligence.
3	Microsoft Security Response Center	The Microsoft Security Response Center (MSRC) investigates all reports of security vulnerabilities affecting Microsoft products and services	*Microsoft*	https://msrc.microsoft.com/update-guide/vulnerability	Go to source for listing CVE's related to microsoft products. Provides exploitability summary and mitigations for each CVE.
4	Microsoft Patches 61 Flaws,	Provides reports and articles about	The Hacker News	https://thehackernews.com/2024/05/mic	The Hacker New stands as a top and

	Including Two Actively Exploited Zero-Days	the latest attacks and vulnerabilities across the cyber landscape.		rosoft-patches-61-flaws-including.html	reliable source for the latest updates in cybersecurity.
5	MOVEit Transfer Seeing Exploit Attempts Via New Critical Vulnerability: Researchers	Discusses the most recent critical MOVEit vulnerability and how it relates to previous attacks on MOVEit.	CRN	https://www.crn.com/news/security/2024/moveit-transfer-seeing-exploit-attempts-via-new-critical-vulnerability-researchers	CRN, a media brand of The Channel Company, is the No. 1 trusted source for IT channel news, analysis and insight
6	NIS2: What it is, how it applies to your business, and what you need to do to prepare	Outlines the new NIS2 Directive and how it compares to the previous directive. Lists the industries it applies to and how to prepare for its introduction.	Risk Ledger	https://riskledger.com/resources/new-nis-2-directive-explained	Risk Ledger is building a global network of connected organisations all working together to defend-as-one. Helping organisations mitigate risks from the supply chain
7	Microsoft's July 2024 Patch Tuesday Addresses 138 CVEs	Discusses monthly microsoft patches relating to software products and their vulnerabilities	Tenable	https://www.tenable.com/blog/microsofts-july-2024-patch-tuesday-addresses-138-cves-cve-2024-38080-cve-2024-38112	Tenable exists to expose and close priority security gaps that put businesses at risk.
8	UK set to debut Cyber Security and Resilience Bill to boost national cyber defences, secure critical	Discusses new UK legislation related to the NIS frameworks.	Industrial Cyber	https://industrialcyber.co/regulation-standards-and-compliance/uk-set-to-debut-cyber-security-and-resilience-bi	Trusted source for UK cyber related news.

	infrastructure			ll-to-boost-national-cyber-defenses-secure-critical-infrastructure/	
9	Cybersecurity laws and legislation (2024 update)	Blog that lists new and updated cybersecurity legislation, primarily in the US.	ConnectWise	https://www.connectwise.com/blog/cybersecurity/cybersecurity-laws-and-legislation	Trusted and leading IT solutions provider