Cybersecurity Watch

Joy Dada
July 2, 2025

Table of contents

1. Executive Summary

This report highlights important cybersecurity updates that relate to some of the key technologies we use at Altergize, including **Windows Server 2019**, **Active Domain Services**, and **MOVEit File Transfer**. These systems are critical to our day-to-day operations, so understanding how they're being targeted—and how we can protect them—is essential.

During this cybersecurity watch, I identified several high-risk vulnerabilities that could seriously impact our network if left unpatched. For example, **CVE-2025-33053** allows attackers to run harmful code just by tricking someone into opening a shortcut file. Another, **CVE-2023-34362**, has been used in real attacks against MOVEit, leading to stolen data from many organizations. These threats show that even older vulnerabilities are still being actively used by hackers.

I also researched two real cyberattacks that are directly related to these systems. One involved a ransomware group called **Cl0p**, which targeted MOVEit servers and stole sensitive data. The second was carried out by a known APT group, **Stealth Falcon**, which exploited the Windows WebDAV vulnerability. Both attacks demonstrate the importance of fast patching, training users to spot risky files, and keeping our systems well monitored.

Lastly, I reviewed two recent updates to cybersecurity laws and frameworks. In the **UK**, the government is introducing the **Cyber Security and Resilience Bill**, which will increase reporting requirements and push companies to better protect their suppliers. In the **U.S.**, CISA is finalizing rules under the **CIRCIA law**, which will require companies like us to report serious cyber incidents and ransomware payments within specific timeframes.

In summary, this cybersecurity watch shows how important it is to stay current on both technical threats and legal requirements. By acting on this information, we can improve our overall security posture, reduce risk, and better protect our systems, data, and reputation.

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-2025-33053	• This vulnerability allows attackers to craft a `.url` file that, when opened, executes code from a remote WebDAV share. It has been exploited by advanced persistent threat groups such as Stealth Falcon and can lead to full system compromise without user interaction. **Severity:** High (CVSS 8.8) **Sources:** ○ Microsoft Security Update Guide: MSRC CVE-2025-33053 ○ CISA KEV Catalog: CISA KEV Entry ○ Check Point Research: APT Exploitation Analysis
Windows Server 2019	CVE-2024-30080	• A vulnerability in Microsoft Message Queuing allows remote code execution via specially crafted HTTP packets. An attacker exploiting this flaw can run arbitrary code on a vulnerable server. **Severity:** Critical **Sources:** ○ Tenable Blog: Patch Tuesday Overview ○ Microsoft MSRC: CVE-2024-30080
Active Domain Services	CVE-2024-38063	Allows an unauthenticated attacker to send specially crafted IPv6 packets to a domain

		controller or server, enabling remote code execution. No user interaction is required, increasing its exploitability. **Severity:** Critical (CVSS 9.8) **Sources:** • Microsoft MSRC: CVE-2024-38063 • The Hacker News: Threat Analysis
Active Domain Services	CVE-2024-38060	An authenticated user can upload a malicious TIFF file to trigger this vulnerability. While admin rights aren't needed, it allows unauthorized execution within the system. Severity: High Sources: • **Microsoft MSRC: CVE-2024-38060**
MOVEit file transfer	CVE-2025-2324	In MOVEit's SFTP module, shared user accounts may gain unintended privileges. This flaw enables lateral movement or unauthorized access to sensitive files by users who should have restricted access. **Severity:** High **Sources:** • Rapid7 Advisory: MOVEit CVE-2025-2324 • NVD Entry: NVD CVE-2025-2324
MOVEit file transfer	CVE-2023-34362	Originally disclosed in 2023, this vulnerability remains under active exploitation in 2025. It allows attackers to execute unauthorized database commands, potentially exposing or modifying confidential data.

		Severity: Critical **Sources:** • The Hacker News: Ongoing MOVEit Exploitation • CISA KEV Catalog: CVE-2023-34362

4. Relevant Cyberattacks

Attack 1: MOVEit Mass Exploitation by Cl0p Ransomware Group (2023–2025)

In May 2023, and continuing into 2025, the **Cl0p ransomware group** exploited a critical SQL injection vulnerability in **MOVEit Transfer** (CVE-2023-34362), a managed file transfer tool used globally by government, finance, healthcare, and energy sectors. The attack allowed the group to gain unauthorized access to MOVEit servers, extract sensitive data, and initiate extortion campaigns. Over 2,500 organizations were affected worldwide, with the breach impacting personal data, intellectual property, and regulated information. This attack represents a **data breach and extortion-style threat**, as Cl0p chose to leak data instead of deploying encryption-based ransomware.

Relevance to Altergize:
Altergize uses MOVEit to transfer sensitive project files and operational data. Given the tool's direct exposure to the internet and role in handling regulated data, vulnerabilities like CVE-2023-34362 represent a major threat to confidentiality and compliance. The continuing scanning and exploitation observed into 2025 also highlights the need for ongoing patching, system hardening, and behavioral monitoring.

Attack 2: Stealth Falcon Exploits Windows WebDAV via CVE-2025-33053

In early 2025, threat intelligence firms reported that **Stealth Falcon**, a state-aligned advanced persistent threat (APT) group, exploited a zero-day vulnerability in **Windows WebDAV** (CVE-2025-33053). The attack leveraged `.url` (Internet Shortcut) files to change the working directory of victim systems and execute malicious code from a remote WebDAV server. This **remote code execution (RCE)** vulnerability allowed attackers to gain unauthorized control of systems without requiring elevated privileges or additional user interaction, making it a stealthy and high-impact method of initial access.

Relevance to Altergize:
Altergize runs Windows Server 2019 and leverages WebDAV components for internal file sharing. Because of the ease of execution and minimal user interaction involved, this vulnerability presents a high risk in environments where `.url` files or shared file systems are common. If exploited, it could allow attackers to establish a foothold in the network, steal data, or disrupt operations—especially in a hybrid or remote-access environment.

5. Security Frameworks and Legislation

1. UK Cyber Security and Resilience Bill (2024–2025)

In 2024, the U.K. government announced the development of the **Cyber Security and Resilience Bill**, which is expected to modernize the existing Network and Information Systems (NIS) Regulations 2018. The bill, as proposed, will expand the scope of regulation to include managed service providers, large cloud infrastructure providers, and other third-party suppliers vital to national resilience. It also aims to shorten incident reporting timelines (from 72 hours to 24 hours for initial notification), establish clearer supply chain obligations, and introduce enhanced powers for U.K. cyber regulators to enforce compliance and conduct audits.

Relevance to Altergize:
Altergize's U.K. operations rely on IT infrastructure, cloud services, and third-party energy tech vendors. This legislation will require the company to bolster incident response processes, document supply chain security measures, and prepare for more frequent compliance checks from U.K. cyber authorities. The bill aligns closely with the EU's NIS2 Directive, signaling a harmonized European cybersecurity landscape.

2. CIRCIA NPRM – U.S. Cyber Incident Reporting for Critical Infrastructure (April 2024)

In April 2024, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) released a **Notice of Proposed Rulemaking (NPRM)** for the **Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)**, originally passed in 2022. The proposed rule mandates that critical infrastructure operators—including those in the energy sector—report substantial cyber incidents within 72 hours and any ransomware payments within 24 hours. Organizations will also be required to preserve data relevant to incidents and cooperate with follow-up investigations. The final rule is expected to be adopted in 2025 following public comment.

Relevance to Altergize:
With U.S.-based energy operations, Altergize will fall under the scope of CIRCIA once it is finalized. The company must begin establishing internal mechanisms to detect, assess, and report qualifying incidents quickly. Implementing streamlined response protocols and aligning with CISA's reporting guidelines will be essential to ensure legal compliance and avoid penalties once enforcement begins.

6. Sources Used for the Report

Sources

Source #	Title of source	Brief description	Publisher	Link	Justification for including source
0 (example)	*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 organizations.*
1	Microsoft Security Update Guide	Lists vulnerabilities in Microsoft products, including CVE details, patches, and severity ratings	Microsoft MSRC	https://msrc.microsoft.com/update-guide	Primary source for Windows Server 2019 and Active Domain Services vulnerabilities
2	The Hacker News – MOVEit Exploitation	Reports on ongoing MOVEit Transfer attacks and exploitation activity	The Hacker News	https://thehackernews.com/2025/06/moveit-transfer-faces-increased-threats.html	Credible source used to explain the real-world attack on MOVEit (Attack 1)

3	CISA KEV Catalog	U.S. government's official list of exploited vulnerabilities	U.S. Cybersecurity & Infrastructure Security Agency	https://www.cisa.gov/known-exploited-vulnerabilities-catalog	An authoritative Government backed and website used to reference actively exploited CVEs (e.g., CVE-2023-34362, CVE-2025-33053)
4	Rapid7 CVE-2025-2324 Analysis	Details on MOVEit shared account privilege escalation vulnerability	Rapid7	https://www.rapid7.com/db/vulnerabilities/progress-moveit-transfer-cve-2025-2324	A credible hub primarily used for vulnerability management, penetration testing and security automation
5	Tenable Patch Tuesday Report (July 2024)	Breakdown of Microsoft vulnerabilities and security updates	Tenable	https://www.tenable.com/blog/microsofts-july-2024-patch-tuesday-addresses-138-cves-cve-2024-30080-cve-2024-38112	Highly credible and trusted website used for vulnerability management and exposure analysis

6	Check Point Research – Stealth Falcon	Report on APT group exploiting CVE-2025-33053	Check Point Research	https://research.checkpoint.com	Credible threat intelligence and cybersecurity research hub used to describe the real-world WebDAV exploit by Stealth Falcon (Attack 2)
7	DLA Piper – UK Cyber Reform Article	Explains the UK's new cybersecurity legislation and its similarities to NIS2	DLA Piper	https://privacymatters.dlapiper.com/2025/04/uk-will-uk-cyber-reforms-keep-step-with-nis2/	A legal-focused resource on data protection and privacy laws around the world
8	Skadden – Cyber Resilience Bill Summary	Legal breakdown of the UK's proposed cybersecurity bill	Skadden	https://www.skadden.com/insights/publications/2025/06/uk-bill-would-increase-cybersecurity	A credible website used for high quality legal insight into cybersecurity and privacy law
9	CISA – CIRCIA NPRM Announcement	Official announcement of U.S. cyber	CISA	https://www.cisa.gov/news-events/news/cisa-release	This is the official resource for cybersecurity alerts for

		reporting rules		s-nprm-circia	US system and beyond

7. Conclusion

This cybersecurity watch report enables Altergize to remain informed, compliant, and resilient. By closely monitoring critical technologies like Windows Server, Active Directory, and MOVEit, we can detect vulnerabilities before they are exploited.
More than just a summary of threats, this report serves as a proactive tool to strengthen the protection of Altergize's systems, employees, and customers.