Altergize

Cybersecurity Watch

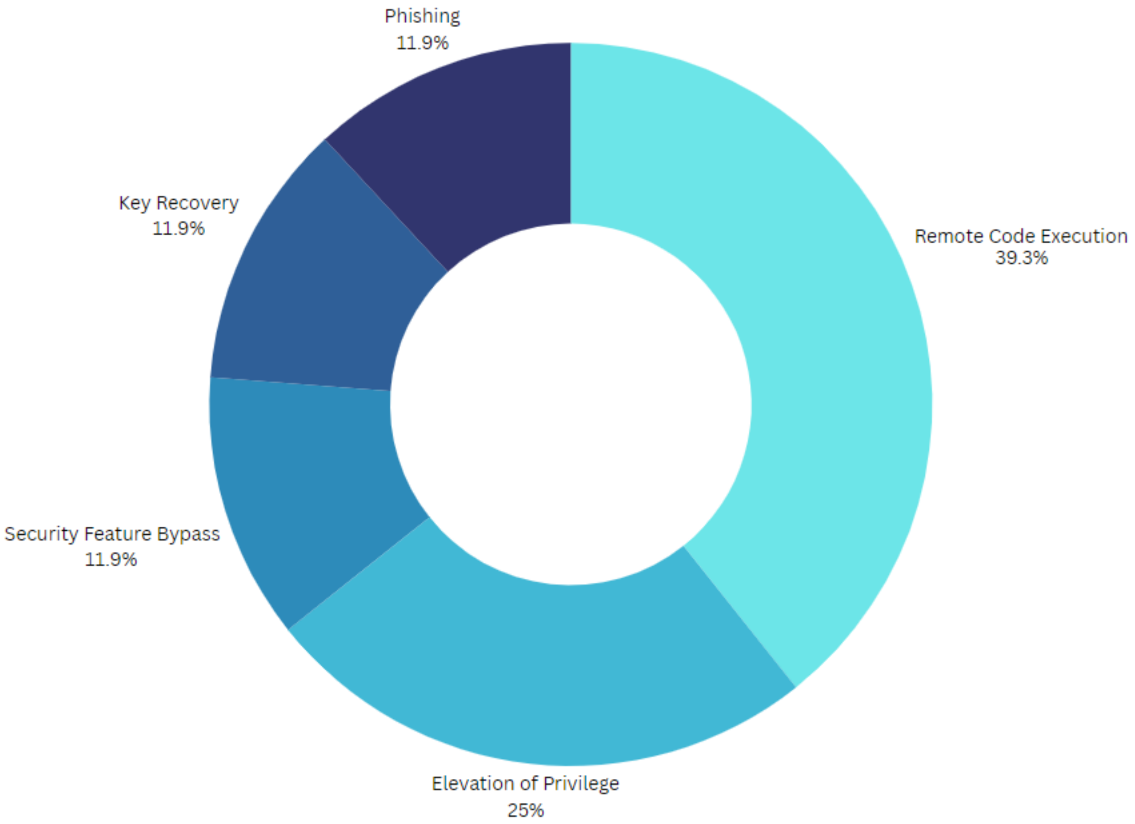
Luis Cruz
10/2024

Table of contents

1. Executive Summary

Our recent security assessment has identified several critical vulnerabilities in key software components within our infrastructure, including Windows Server, Windows Active Domain Services, and MOVEit file transfer. These vulnerabilities pose significant risks to our systems security and could potentially lead to data breaches, unauthorized access, and operational disruptions.

The chart shows the distribution of vulnerability types among the identified vulnerabilities.



Vulnerabilities were evaluated with three critical vulnerabilities to be aware of:

- **Windows - CVE-2024-43572 (Microsoft Console Remote Code Execution Vulnerability):** This vulnerability has a CVSS score of 7.8, indicating a high severity level. It is actively exploited and allows attackers to potentially take complete control of affected systems.
- **MOVEit - CVE-2024-5806 (MOVEit Transfer Improper Authentication):** This vulnerability has a CVSS score of 9.1, which is critical. It allows attackers to bypass authentication mechanisms and gain unauthorized access to sensitive data.
- **Windows Server 2019 - CVE-2024-43491 (Windows Server 2019 Servicing Stack Vulnerability):** This vulnerability can potentially reinstate previously mitigated vulnerabilities on specific Windows 10 versions if left unpatched. While it doesn't affect newer versions, it's still critical for unsupported systems.

Other vulnerabilities found were CVE-2024-38100 Windows Server 2019, CVE-202431497 FileZilla Key Recovery, and CVE2024-38112 Active Domain Services

Key Findings:

- **Remote Code Execution (RCE):** RCE vulnerabilities accounted for a significant portion of Microsoft's July patches, highlighting their criticality.
- **Elevation of Privilege (EoP) and Security Feature Bypass:** These vulnerabilities can allow attackers to gain unauthorized access or bypass security controls.
- **Vulnerabilities exist in widely used software:** The affected software components are essential to our infrastructure, making these vulnerabilities particularly concerning.

Regulatory Landscape and Implications:

- **Global cybersecurity initiatives:** The NIS2 Directive, CSR Bill, and FISMA overhaul underscore the increasing importance of cybersecurity for critical infrastructure.
- **Mandatory incident reporting and expanded scope:** These regulations will require organizations to report incidents and adhere to stricter security standards.
- **Focus on governance and supply chain security:** The NIST Cybersecurity Framework 2.0 emphasizes the need for robust governance and risk management practices.

Recommended Actions:

1. **Prioritize patching:** Immediately address these critical vulnerabilities by applying the latest security updates from Microsoft and other vendors.
2. **Review and strengthen security controls:** Implement robust security measures to prevent exploitation of these vulnerabilities, such as network segmentation, access controls, and regular vulnerability assessments.
3. **Stay informed about emerging threats:** Monitor the threat landscape and be aware of new vulnerabilities that may affect your systems.
4. **Adhere to regulatory requirements:** Ensure compliance with relevant cybersecurity regulations, such as NIS2, CSR Bill, and FISMA.
5. **Focus on governance and supply chain security:** Implement a robust governance framework and manage supply chain risks to enhance overall security posture.

By taking proactive steps to address these critical vulnerabilities and comply with emerging regulations, we can significantly reduce the risk of security breach, protect our organization's valuable assets, and maintain our reputation in the renewable energy sector.

2. Identified Technologies

These software components were chosen for the cybersecurity watch due to their criticality:

Windows Server 2019
Windows Active Domain Services
FileZilla Server for Windows
MOVEit file Transfer

3. High-Impact Vulnerabilities

Technology	**Vulnerability (CVE-ID)**	**Brief description of the vulnerability**
Windows Server 2019	*CVE-2024-43491 Remote Code Execution*	Can reinstate previously mitigated vulnerabilities on specific Windows 10 versions.
Windows Server 2019	CVE-2024-43572 Remote Code Execution	Allows attackers to execute arbitrary code on affected systems.
Windows Server 2019	CVE-2024-38100 Improper Access Control	Allows attackers to escalate privileges on a Windows system.
MOVEit	CVE-2024-5806 Authentication Bypass	Can allow attackers to bypass authentication and gain unauthorized access.
FileZilla Key Recovery	CVE-2024-31497 Key Recovery	Affects older versions of FileZilla and could allow attackers to recover user secret keys.
Active Domain Services	CVE-2024-38112 Platform Spoofing	Could allow attackers to trick users into opening malicious files.

4. Relevant Cyberattacks

Our analysis has identified three critical vulnerabilities that could have significant consequences for Altergize and its operations: CVE-2024-43572, CVE-2024-5806, and CVE-2024-43491. These vulnerabilities, if exploited, could allow attackers to gain unauthorized access to our systems, execute malicious code, or compromise sensitive data. While these vulnerabilities have been patched, it is imperative that we ensure all company systems are receiving regular updates to prevent future attacks that could exploit similar vulnerabilities.

Attack 1: Windows - CVE-2024-43572
Remote Code Execution (RCE) (CVSS: 7.8)

Researchers at Elastic Security Labs disclosed an attack technique called GrimResource that leveraged an old cross-site scripting (XSS) vulnerability combined with a specially crafted Microsoft Saved Console (MSC) file to gain code execution privileges. Successful exploitation would allow the attacker to execute arbitrary code.

Attack 2: MOVEit - CVE-2024-5806
Authentication Bypass (CVSS: 9.1)

Discovered in June 2024 by Progress Community, this vulnerability allows attackers to bypass authentication and gain unauthorized access to a MOVEit Transfer server, potentially leading to data breaches and operational disruptions. The widespread use of MOVEit Transfer has made this vulnerability a significant threat to organizations across various industries.

Attack 3: Windows - CVE-2024-43491
RCE/Previous Patch Bypass (CVSS: 9.8)

Microsoft is aware of a vulnerability in Servicing Stack that has rolled back the fixes for some vulnerabilities affecting Optional Components on Windows 10. Attackers exploiting this flaw can undo previously applied patches, potentially leaving systems exposed to vulnerabilities that were thought to be resolved. The flaw is linked to the Windows Servicing Stack, which manages how updates are applied, particularly affecting Optional Components. Attackers can exploit this flaw to reintroduce vulnerabilities from previous updates, making patched systems once again vulnerable to known threats. Attackers can undo important previously implemented security patches leaving Altergize systems open to a variety of risks.

5. Security Frameworks and Legislation

The cybersecurity landscape is evolving rapidly, with new regulations and frameworks emerging to address increasing cyber threats. In the UK and U.S., recent updates to existing legislation and the introduction of new frameworks aim to strengthen cybersecurity across critical sectors, including renewable energy.

In the UK, the Cybersecurity and Resilience (CSR) Bill, announced in July 2024, seeks to expand upon the existing Network and Information Systems (NIS) Regulations. The NIS 2 Directive, introduced in December 2022, also imposes more stringent security requirements on operators of essential services. Both initiatives emphasize the need for robust cybersecurity frameworks to safeguard against potential disruptions and cyber threats.

In the United States, the recent overhaul of the Federal Information Security Modernization Act (FISMA) aims to improve federal agencies' cybersecurity postures and foster better coordination across government bodies. Additionally, the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0 provides a comprehensive guide for organizations to implement effective cybersecurity measures.

These regulatory developments highlight the increasing importance of cybersecurity for critical infrastructure. Organizations must now adhere to stricter requirements for incident reporting, governance, and supply chain security. By understanding and implementing these frameworks, businesses can better protect themselves against cyber threats and ensure the continuity of their operations.

6. Sources Used for the Report

Sources

Source #	Title of source	Brief description	Publisher	Link	Justification for including source
1	*CISA adds three known exploited vulnerabilities to catalog.*	***CISA is a crucial resource for organizations seeking to improve their cybersecurity posture and protect themselves from cyber threats.***	*CISA*	*https://www.cisa.gov/news-events/alerts/2024/10/08/cisa-adds-three-known-exploited-vulnerabilities-catalog*	*The CISA is a federal agency that protects critical infrastructure from cyber threats.*
2	Microsoft Windows Update Remote Code Execution Vulnerability	MSRC provides vulnerability research, patch development, customer support and threat intelligence. To help protect Microsoft products and customers from security threats.	Microsoft	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43491	Dedicated team within Microsoft responsible for handling security threats and vulnerabilities related to Microsoft products.
3	Windows File Explorer Elevation of Privilege Vulnerability	NIST offers cybersecurity services such as the NIST Cybersecurity Framework and standards for protecting sensitive data, helping organizations improve their security posture.	NIST	https://nvd.nist.gov/vuln/detail/CVE-2024-38100 https://nvd.nist.gov/vuln/detail/CVE-2024-31497	A respected and reliable source for cybersecurity information due to its government affiliation, technical expertise, objectivity, collaboration, and widespread recognition.
4	5 Zero-Days in Microsoft's October Update to	News and Analysis, publishing daily news articles, blog posts and research	Dark Reading	https://www.darkreading.com/vulnerabilities-	Cybersecurity news and information website that

	Patch Immediately	reports.		threats/5-cves-microsofts-october-2024-update-patch-now	offers a wide range of services for security professionals and organizations.
5	MOVEit Transfer Critical Security Alert Bulletin	A resource that provides information about security vulnerabilities and updates related to the MOVEit Transfer Software.	Progress Community	https://community.progress.com/s/article/MOVEit-Transfer-Product-Security-Alert-Bulletin-June-2024-CVE-2024-5806	Online platform and community forum dedicated to users of Progress software products.
6	Patch Tuesday	Site provides Investigative Journalism, Breaking News, Expert Analysis, and Community Engagement.	Krebs on Security	https://krebsonsecurity.com/2024/10/patch-tuesday-october-2024-edition/	Prominent cybersecurity blog & news site founded by Brian Krebs. It is dedicated to providing in-depth coverage of cybersecurity threats, vulnerabilities& incidents.
7	Microsoft's October 2024 Patch Tuesday Addresses 117 CVEs	Monthly security release cycle where Tenable releases new patches and security updates for Microsoft products.	Tenable	https://www.tenable.com/blog/microsoft-october-2024-patch-tuesday-addresses-117-cves-cve-2024-43572-cve-2024-43573	Tenable exists to help organizations protect themselves from cyber threats
8	Windows 10 Security Vulnerability	Strong reputation in the cybersecurity industry with a variety of product offerings that can help organizations	TrueFort	https://truefort.com/cve-2024-43491-windows-10-security-vulnerability/	Well established cybersecurity company that provides a range of services, including vulnerability

		improve their data posture.			management, threat intelligence, & compliance solutions.
9	Detect exploitation by Void Banshee APT in Zero-Day Attacks targeting Windows users.	SOC Prime offers a platform for threat intelligence sharing and detection, enabling organizations to improve their security posture.	Soc Prine	https://socprime.com/blog/detect-cve-2024-38112-exploitation-by-void-banshee-apt-in-zero-day-attacks-targeting-windows-users/	It is a well-established cybersecurity company that provides a platform for threat intelligence sharing and detection.
10	United States International Cyberspace & Digital Policy Strategy	Focuses on promoting digital solidarity, building partnerships, and countering malicious cyber activity.	U.S. Department of State	https://www.state.gov/united-states-international-cyberspace-and-digital-policy-strategy/	Credible source due to its role as a leading global actor in cybersecurity and its commitment to promoting international cooperation and collaboration.
11	**Cybersecurity rules saw big changes in 2024. Here's what to know**	Global organization that brings together leaders from business, government, civil society, and academia to address global challenges.	World Economic Forum	https://www.weforum.org/agenda/2024/10/cybersecurity-regulation-changes-nis2-eu-2024/	Often publishes reports and analyses on cybersecurity topics. Facilitates collaboration among governments to address cybersecurity topics.