Altergize

Cybersecurity Watch

Darius Richardson

11/08/2024

Table of contents

1. Executive Summary

The purpose of this report is to be able to identify the high impact vulnerabilities from other organisations that are applicable to the software and technology used in Altergize by researching the latest news, blogs and reports of these cyberattacks whilst monitoring any updates to learn more about what is happening and to prevent any potential cyberattacks in Altergize.

The resources collected throughout the report has provided detailed information to make a judgement as to why the software has been chosen and what types of cyberattacks impact the software that are relevant to the company. This includes ransomware, hacking and Denial as a service. The resources that are gathered are reliable and credible as they come from big organisations such as Microsoft and the NHS as well as backed up by other sources to prove its reliability.

The software's chosen are Windows Server 2019, MOVEit Secure Managed File Transfer Software, Fortinet VPN SSL and Active Directory Certificate Services. The Windows Server 2019 is important for ensuring that the centralised resource or service in a network is secure. MOVEit secure managed file transfer software is critical when protecting the data from clients and customers. The Fortinet VPN SSL is important when protecting the network's security system from attacks and Active Directory Service is important for an organized way to manage and control access to resources within a network.

The reason these software have been chosen rather than the other software is because they were more important and based on research and data they have more vulnerabilities which means they a more likely to be tampered with and requires more attention. The (CVE-ID) detects the number of vulnerability of the software of that year for example CVE-2024-5806 meaning that there are 5806 vulnerabilities in 2024. This can help to determine which software has the most vulnerability when it comes to cyberattacks.

These software's that have been chosen were based on research to make sure that it is understandable on how the software is used in other organisations and how they protect these software's from cyberattacks as a way to learn from them. All information that is gathered relates to the green energy company Altergize.

Also, researched on updated frameworks applicable to the UK and US will help in protecting the security of the infrastructure and help prevent customer data from being stolen for financial gain. The frameworks discussed in this report for the United Kingdom and the United States are the latest frameworks to help protect the systems that is used to secure the data of Altergize. The sources are from reliable sources that mentions NIST and CIS frameworks. The CIS framework provides latest updates and reflects on emerging threats and technologies. The NIST framework provides continuous vulnerability management and control access to systems which can make sure that hackers cannot cause harm to the systems.

It is important to always stay updated on future cyberattacks to protect Altergize. Technology such as Artificial intelligence continues to grow and it gives attackers the advantage to use technology to cause significant harm to a company such as deepfake which uses Artificial Intelligence and machine learning to allow someone to pretend to be someone else. So it critical to stay updated on technology to prevent any cyberattacks from happening or to minimise the attacks.

2. Identified Technologies

The following software programs were selected for the Cybersecurity watch:

Windows Server 2019.
MOVEit Secure Managed File Transfer Software.
Fortinet VPN SSL.
Active Directory Certificate Services.

3. High-Impact Vulnerabilities

Technology	**Vulnerability (CVE-ID)**	**Brief description of the vulnerability**
Windows Server 2019	CVE-2024-38074	**1.** An attacker with site owner privileges can execute arbitrary code in the context of Share Point Server by uploading specially crafted files to the target Share Point Server and making specialized API requests that trigger deserialisation of file parameters. As a result, it will tamper with the server preventing data from going through the network. **2.** An attacker with ordinary user rights can upload malicious TIFF files to the server. The consequences of this will mean that the attacker will steal all kinds of data from the organisation in the process.
MOVEit Secure Managed File Transfer Software	CVE-2024-5806	**1.** Internet-facing MOVEit Transfer servers were targeted by multiple threat groups including the cybercriminal group associated with CL0P ransomware in a mass-exploitation campaign affecting hundreds of victim organisations, resulting in major disruption and data loss which could cause a negative impact on the organisation's reputation. **2.** The CVE-2024-5805 relates to an improper authentication issue in Progress in MOVEit Gateway's SFTP modules, allowing for an authentication bypass. The consequences will be for hackers to be able to gain access to an application, service or device.
Fortinet VPN SSL	CVE-2024-21762	**1.** The SSL VPN functionality of Fortinet's FortiOS. It's classified as an out-of-bound write vulnerability. In simpler terms, it's can relate to a hidden flaw in a network's security system. The consequences of this is potentially allowing unauthorised external access such as security incident. **2**. Fortinet VPN SSL allow a remote unauthenticated attacker to execute arbitrary code or command via specially crafted HTTP requests. The consequences of this is information leakage and cache poisoning as an attempt to harm users.
Active Directory Certificate Services	CVE-2024-38080	**1.** The main vulnerability of the active directory certificate services are hackers that can exploit unpatched applications. The consequences for this is significant financial and reputational damage to the organisation. **2.** Another main vulnerability would be the AD Services that could target passwords resulting in the hacker being able to access sensitive data which could lead to loosing customer trust.

4. Relevant Cyberattacks

Attack 1:

In 2023, the Clop ransomware group attacked MOVEit Transfer, a secure managed file transfer software to rob its customers' sensitive data using ransomware. This has impacted 255 organisations. The ransomware attack is relevant to Altergize because the company also uses MOVEit Secure Managed File Transfer Software and could potentially cause a serious problem with the customers data being compromised and the infrastructure being tampered bringing about operational disruption. The reference for the source is from Kolide blog written by Kenny Najarro. The reason for choosing the source is because the blog provides factual information from a variety of reliable sources such as Progress Community. Judging based on the attack is that the motivate behind this attack is cyber espionage and financial gain. There are also malware done by embedding code in an inverter which causes the malware to spread into larger power systems and other cyberattacks that can also cause harm to energy solutions such as solar panels, wind energy, hydroelectric power and energy storage systems that Altergize uses so its important they are protected.

Attack 2:

In September 2023, Microsoft was altered by industry partners about Distributed Denial-of-Service (Ddos) attack technique attacking HTTP/2 protocol. This vulnerability impacts any internet exposed to HTTP/2 endpoints. HTTP/2 servers have been targeted from the attacker by setting a number of HTTP requests using HEADERS following by RST_STREAM and repeating this pattern to generate a high volume of traffic. The purpose of the attacker is a cyber espionage. The reason for choosing the source is because it comes from a well known company with references from other sources that proves its credibility. By understanding the severity of the attack it is crucial to make sure the Windows Server 2019 for Altergize is secure to prevent this attack from happening. It's important to gather information and data to better understand and anticipate cyber threats as well as to provide insight into the motivates and methods of the attacker this is known as Cyber Threat Intelligence.

5. Security Frameworks and Legislation

A recent update from the last year is the Centre for Internet Security Controls framework that is applicable to the United Kingdom. It is best at protecting against information systems and data from cyber threats. This can relate to the company making sure the Windows Server 2019 is secure to prevent data lost. The framework controls various aspects of cybersecurity such as inventory and control of software and hardware assets. This helps in dealing with incident response to make sure that incidences are dealt with straight-away. This will help with the energy company Altergize for the United Kingdom as it will identify new vulnerabilities on its identified systems to be able to resolve the issue quickly. The framework can help with securing the network for the Fortinet VPN SSL by making sure that it is secure and the network range is the signal it is able to communicate effectively and Active Directory Certificate Services is crucial to making sure that the Altergize systems are protected and the software application used is protected from attackers.

Another recent update from last year is the NIST Cybersecurity Framework (CSF) that is applicable in the United States. It makes it easier to put the CSF into practice for all organisations. Changes that have be made in the newest version framework compared to the older version is the expanded scope and expanded guidance on implementing the CSF. This will help to identity the vulnerability of the systems. This applies to Altergize as this can help protect from new vulnerabilities on Altergize’s systems by expanding the scope of the security control’s guidance.

6. Sources Used for the Report

Sources	Title of source	Brief description	Publisher	Link	Justification for including source
0	Solar Cybersecurity Basics.	Explains about how hackers use cyberattaks to cause harm solar panels.	Solar Energy Technologies Office.	https://www.energy.gov/eere/solar/solar-cybersecurity-basics#:~:text=An%20attacker%20could%20also%20embed,as%20well%20as%20financial%20damage.	A reliable source from the office of Energy Efficient and Renewable energy that talks about the continuous risk management of solar power systems.
1	Security Update Guide.	Explains the vulnerabilities of the software and technologies as well as the level of severity.	Microsoft.	https://msrc.microsoft.com/update-guide/vulnerability	Microsoft is a reliable source providing details about the vulnerabilities and level of severity.
2	Microsoft's Security Update in July of High-Risk Vulnerabilities in Multiple Products.	The vulnerabilities of servers and an update to resolve them.	NSFOCUS.	https://nsfocusglobal.com/microsofts-security-update-in-july-of-high-risk-vulnerabilities-in-multiple-products/	This source provides factual and detailed information about a range of multiple servers including Microsoft Server 2019. Credible by a Chinese company.
3	Progress Software Releases Critical Security Updates for MOVEit Transfer and MOVEit Gateway.	The two improper authentication vulnerabilities of MOVEit Secure Managed File Transfer Software.	NHS	https://digital.nhs.uk/cyber-alerts/2024/cc-4516#:~:text=MOVEit is a managed secure,authentication bypass in MOVEit Transfer.%0D%0A	This resource is authoritative that provides detailed information about the vulnerabilities of MOVEit Secure Managed File Transfer Software which is relevant to Altergize as they use the same software.
4	Critical Out-of-Bounds Write Vulnerability CVE-2024-21762 in FortiOS and FortiProxy.	Report of the remote unauthenticated attacker in FortiOS and FortiProxy SSL-VPN devices.	NHS Digital.	https://digital.nhs.uk/cyber-alerts/2024/cc-4452	This source provides information about the vulnerability of FortiOS. FortiProxy and FortiProxy SLL-VPN devices which is crucial for Altergize as it uses Fortinet VPN SSL.

5	Understanding CVE-2024-21762: a critical vulnerability in Fortinet’s FortiOS.	Report of vulnerability in Fortinet’s FortiOS.	Claranet.	claranet.com/uk/blog/understanding-cve-2024-21762-critical-vulnerability-fortinets-fortios#:~:text=What%20is%20CVE-2024-21762,potentially%20allowing%20unauthorised%20external%20access.	The source helps provide information about the flaws in the network security system. Clarent is an IT service management company.
6	MOVEit Hack: the Ransomware Attacks Explained.	Report of Ransomware attack for MOVEit Hack.	Kenny Najarro.	https://www.kolide.com/blog/moveit-hack-the-ransomware-attacks-explained	This blog provide details of Ransomware attack will help Altergize to protect its MOVEit Secure Managed File Transfer Software.
7	MOVEit Transfer Critical Vulnerability (May 2023) (CVE-2023-34362).	The vulnerabilities of of the MOVEit Secure Managed File Transfer Software.	Progress Community.	https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023	Very detailed documentation that references reliable sources.
8	Microsoft Response to Distributed Denial of Service (DDoS) Attacks against HTTP/2.	Attacks against HTTP/2 using Distributed Denial of Service.	Microsoft.	https://msrc.microsoft.com/blog/2023/10/microsoft-response-to-distributed-denial-of-service-ddos-attacks-against-http/2/	The resources comes from a reliable company and has provided researched resources.
9	Introducing Active Cyber Defence 2.0	Blog post the Cyber Defence 2.0	Ollie Whitehouse and Jonathon Ellison.	https://www.ncsc.gov.uk/blog-post/introducing-active-cyber-defence-2	The resources provides detailed information on help to provide secure services.
10	Understanding & Mitigating Exploitation Risks in Active Directory Certificate Services (AD CS).	Provides the risks in active directory certificate services.	Doug Bigalke.	https://www.secureideas.com/blog/understanding-and-mitigating-exploitation-risks-in-active-directory-certificate-services-ad-cs#:~:text=To%20address%20these%20risks%2C%20organizations,safeguarding%20against%20these%20potential%2	This resource provides updates in real time and is backed up by reliable resources to provide its credibility. Also, the course was written by an author who has experience as a security consultant.

				0vulnerabilities.	
12	How European countries are implementing new cybersecurity framework.	European countries are going to install a new cybersecurity framework.	Alina Clasen.	https://www.euractiv.com/section/cybersecurity/interview/how-european-countries-are-implementing-new-cybersecurity-framework/	This news article was written by an experienced author and is represented by the EU. The Euractiv is a European news website that provides factual information.
13	Cybersecurity Frameworks to help reduce Cyber risk.	Resource about the latest frameworks including the centre for internet security control framework in the United Kingdom.	Core To Cloud.	https://www.coretocloud.co.uk/frameworks/	This will help Altergize provide a secure framework which will be reliable to the company help protect information systems and data from cyber threats.
14	NIST Releases Cybersecurity Framework 2.0 Draft & Implementation Examples.	Report on the releases of Cybersecurity Framework 2.0 in the United States.	NIST.	https://csrc.nist.gov/News/2023/nist-releases-cybersecurity-framework-2-0-draft#:~:text=August%2008%2C%202023&text=After%20reviewing%20more%20than%20a,help%20organizations%20reduce%20cybersecurity%20risk.	The resource provide the latest update when comes to framework and provides guidance on implementing the CSF. National Institute of Standards and Technology is a reliable source due to it being a Government agency.