Mitigating Windows Server Vulnerabilities

Ethan Lasich

Old Dominion University

CYSE 280: Windows System Management and Security

Professor Malik A. Gladden

23 November 2025

Introduction

Microsoft Windows Server has been around since 1993, and has been one of the go-to platforms for enterprise environments since its release. While Linux servers are used for the majority of web traffic, one source reports that “In 2024, the Windows segment held a dominant market position, capturing a 52.6% share of the Global Server Operating System Market.” (market.us, 2024), which is largely due to its user-friendly interface and its ability to support the needs of business environments through strong application support and constant security updates. However, such widespread adoption opens many opportunities for malicious actors looking to make money or bring chaos by targeting the Windows Server operating system. At the same time, cyber threats have been increasing for many years, and many organizations face challenges with patching these threats mitigating human factors through security awareness and employee phishing. Due to these threats, security vulnerabilities in Windows environments remain one of the most critical concerns for modern business and require a thorough understanding and proactive management in order to mitigate risk and strengthen the security posture of enterprise environments.

Overview of Research / Required Information

Before looking at frameworks and tools to mitigate these vulnerabilities, it’s important to understand what risks exist in the Windows Server environment and how they are exploited by hackers. One of the most dangerous vulnerabilities for any systems are called zero day exploits, which are vulnerabilities that are only known to a hacker, meaning security researchers and organizations don’t know of their existence and therefore have no patches to prevent these attacks. Zero days have historically been used to target end users, however Google Threat Intelligence Group has found that zero days are being used more frequently in enterprise environments than ever before, posing even more of a threat than just a couple years ago. According to GTIG's data, they "spotted 95 zero-days, and 71 of them were deployed against user systems like browsers and smartphones. In 2024, 33 of the 75 total vulnerabilities were aimed at enterprise technologies and security systems. At 44 percent of the total, this is the highest share of enterprise focus for zero-days yet." (Whitwam, 2025). Other common vulnerabilities in Windows environments include failing to patch applications in time, and using outdated protocols such as SMBv1 and NTLM. These trends make it clear that Windows Server environments are becoming more targeted by zero-days than ever.

Another significant risk in Windows Server environments are misconfigurations of privileges and services that give opportunities to hackers that would otherwise be unavailable in properly secured environments. According to a Crowdstrike blog, some of the most abused misconfigurations include administrative privileges for all users, open network shares, weak passwords, old accounts, and using legacy systems (Smith & Moser, 2021). To elaborate, not disabling admin privileges on users accounts allows attackers to immediately start installing backdoors, modifying settings, and disabling security controls, without ever needing to move laterally to other machines or escalate their privileges, a time consuming process that is likely to be caught. Additionally, open network shares can expose sensitive files to the open internet, while weak or reused passwords make brute force or dictionary attacks far easier to use. Unused accounts also pose a risk because they are usually not known about or unmonitored, giving attackers an easy entry point, and finally using legacy systems or outdated versions of Windows Server poses a significant risk by introducing vulnerabilities that Microsoft no longer patches. Together all these misconfigurations can expand the attack surface of Windows Server Environments and make them more vulnerable than necessary.

In addition to zero days and misconfigurations, human based security weaknesses also pose a significant threat to Windows Server environments. One of the most common security weaknesses for any platform stem from social engineering, which is when an attacker tricks another person into giving them information or access into a network. This is usually done through what are called phishing attacks, which are most commonly sent by email and trick users into clicking a malicious link. This link could either be a fake version of a website that a user will login to, giving the hacker their password, or it could just infect their computer with malware and give full access to the device. Tomer Shloman from trellix.com explains that phishing works because it exploits the trust of humans, which can't be controlled as easily as technical solutions like firewall rules or ACLs. It also sometimes makes the user think the email they're reading comes from a figure of authority like a boss or CEO, and "The principle of authority leverages the human tendency to comply with requests from authority figures without question." (Shloman, 2024).

Frameworks / Processes to follow / Methodology

In order to mitigate these vulnerabilities within Windows Servers, there are many best practices that can be followed, as well as robust security frameworks that serve as a guide for hardening Windows environments. One of the most well known frameworks is called the NIST Cybersecurity Framework, which is structured into six different functions: identify, protect, detect, respond, recover, and govern. According to their documentation, the guidelines are "designed to help organizations of all sizes and sectors — including industry, government, academia, and nonprofit — to manage and reduce their cybersecurity risks." (nist.gov, 2024). Another valuable set of frameworks that can be referenced are the CIS benchmarks, created by the Center for Internet Security. These benchmarks are "internationally recognized as security standards" that are "used by thousands of businesses" and provide information on the best practices and baselines for securely configuring systems (microsoft.com, n.d.). CIS also provides hardened images, which are virtual machine images for many operating systems, including Windows Server 2019 and 2022, which are preconfigured to meet their benchmark standards and protect against many weaknesses that default Windows setups are vulnerable to.

Aside from frameworks, there are also many processes that can be followed to protect Windows Server from common security vulnerabilities. The first one is implementing a least privilege architecture, which means giving users the least amount of access and permissions on a computer necessary to perform their work. This is best handled with role-based access control and ensures that if an attacker were to take over a computer, the amount of damage they can cause will be limited. Another best practice is to implement strong password policies, creating rules for password length, complexity, and maximum password age. The University of Connecticut recommends setting passwords to a minimum length of 8 characters and having them expire after 90 days. They also recommend having accounts be locked for 15 minutes after 10 failed login attempts (uconn.edu, n.d.). These settings assure that if a hacker has access to a locked computer, there's no way for them to brute force password attempts to get in. Additionally, patching applications and updating Windows Server is another important best practice, as these patches provide security updates for known vulnerabilities, and running older versions of software and operating systems leaves Windows open to attacks. These patches should also be tested in a simulated environment before applying it to the whole network, making sure that it doesn't cause any conflicts with other services running on the system. One important thing to note about Windows updates is that Microsoft pushes security patches on a predictable schedule called Patch Tuesday, which occurs on the second Tuesday of each month.

One source found that on the most recent Patch Tuesday, “Microsoft this week pushed security updates to fix more than 60 vulnerabilities in its Windows operating systems and supported software, including at least one zero-day bug that is already being exploited.” (Krebs, 2025). This high number of patched vulnerabilities emphasizes the importance of keeping systems up to date, as failing to apply them in a timely manner leaves Windows environments exposed to weaknesses that attackers are already exploiting.

Tools / Resources

In addition to following best practices, implementing security tools and programs into Windows that help with computer hardening is another highly effective step in weakening the effectiveness of vulnerabilities. The most common security tools are antiviruses, and there’s one that’s built right into Windows Server called Windows Defender. This is a free tool that can be used to scan a computer for malware or other suspicious files, and also provides real time protection to stop malicious code from executing in the first place. It also comes with a built-in software firewall, to defend Windows against malicious inbound traffic or attempts by attackers to probe open ports and services. There are also many paid alternatives to Windows Defender such as Kaspersky or Bitdefender, which offer advanced threat protection and behavioral analysis that could appeal to organizations with more complex security needs. With malware being one of the most common ways to exploit Windows vulnerabilities, having strong endpoint protection is a must have for server hardening.

Another commonly used security tool to protect Windows Server are vulnerability scanners. Some of the most popular programs include Nessus and Openvas, and they work by employing “a variety of techniques to identify vulnerabilities, including network scanning, port scanning, service enumeration, and vulnerability checks based on extensive plugins. These plugins contain checks for thousands of known vulnerabilities across diverse platforms and applications.” (Yen, 2024). By using vulnerability scanners, security flaws can be easily discovered and patched, which is especially valuable for Windows when new vulnerabilities are always being found and manual monitoring isn’t very realistic.

Finally, one more powerful tool that can significantly reduce the risk of vulnerabilities is Security Information and Event Management, or SIEM for short. A SIEM collects log data from workstations, Windows servers, programs, and networking equipment, correlates and analyzes the data for anomalies. When it detects something unusual, it will send an alert that allows admins to investigate the issue before it becomes a security concern. One source emphasizes the importance of SIEM’s by noting “the average organization’s security operations center (SOC) receiving more than 10,000 alerts per day, and the biggest enterprises seeing over 150,000, most enterprises do not have security teams large enough to keep up with the overwhelming number of alerts.” (fortinet.com, n.d.). Without any way of managing all these alerts, critical threats could easily be overlooked and allow attackers to exploit vulnerabilities, but a SIEM mitigates this by filtering and prioritizing alerts, allowing Windows admins to focus on the most important issues first.

Conclusion / Results

In conclusion, this research shows that Windows Server security vulnerabilities have a significant impact on enterprise environments, and pose a major threat to the operation and reputation of organizations. Things like zero-days, misconfigurations, outdated protocols, and human based threats have all been on the rise and pose major risks to organizations that can be exploited by attackers, and without understanding what tools and procedures are effective against these threats, it can be difficult to mitigate them. My research finds that enterprises that adopt frameworks like NIST and CIS, follow best practices like least privilege and strict patch management, and also utilize tools like antiviruses, vulnerability scanners and SIEMs, are better prepared to prevent breaches and reduce the risk that vulnerabilities pose to Windows Server environments. Overall, this paper emphasizes that organizations should focus on understanding, monitoring, and mitigating Windows Server vulnerabilities, as it is crucial to protect businesses from the growing risk of cyber attacks.

Works Cited

Fortinet. (n.d.). *SIEM for Enhanced Security: How It Detects & Manages Threats*. https://www.fortinet.com/resources/cyberglossary/what-is-siem

Krebs, B. (2025, November 16). Microsoft Patch Tuesday, November 2025 Edition. https://krebsonsecurity.com/2025/11/microsoft-patch-tuesday-november-2025-edition/

Market.us. (2025, September). *Server operating system market trend | CAGR of 11.2%.* https://market.us/report/server-operating-system-market/#:~:text=adoption%20accelerates%20globally.-,Operating%20System%20Analysis,scale%20enterprises%20across%20diverse%20industries

Microsoft. (n.d.). *CIS benchmark offerings for Windows Server*. https://learn.microsoft.com/en-us/compliance/regulatory/offering-cis-benchmark

National Institute of Standards and Technology. (2024, February 26). *NIST Cybersecurity framework: Overview*. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Shloman, T. (2024). *The Psychology of Phishing: Unraveling the Success Behind Phishing Attacks and Effective Countermeasures* Trellix. https://www.trellix.com/blogs/research/understanding-phishing-psychology-effective-strategies-and-tips/

Smith, S., & Moser, J. (2021, February 4). *Seven common Microsoft AD misconfigurations that adversaries abuse*. CrowdStrike.

https://www.crowdstrike.com/en-us/blog/seven-common-microsoft-ad-misconfigurations-that-adversaries-abuse/

University of Connecticut. (n.d.). *Server hardening standard: Windows*. https://security.uconn.edu/server-hardening-standard-windows/

Whitwam, R.. (2025, April 29). *Google: Governments are using zero-day hacks more than ever*. Ars Technica. https://arstechnica.com/security/2025/04/google-governments-are-using-zero-day-hacks-more-than-ever/

Yen, L. (2024, February 23). *OpenVAS vs. Nessus: Top Vulnerability Scanners Compared* https://www.datamation.com/security/openvas-vs-nessus/