Role of Patch Management in Securing Windows Environments

Zyron James M. Sumulong

Old Dominion University

CYSE 280: Windows System Management and Security

Dr. Malik A. Gladden

December 1, 2025

Introduction

Windows operating systems have remained at the center of enterprise technology infrastructures, powering workstations and servers, authentication services, and critical business applications across nearly every industry. As of July 2024, Windows has continued to support more than 68 percent of all enterprise desktops worldwide, with just over 1 billion active devices serving as the backbone for both local and cloud-to-cloud workflows (Bhalla, 2025). With this support comes numerous and great significant challenges; Windows systems remain the most frequently targeted platforms for cybersecurity attacks. Threats ranging from sly cybercriminals to highly sophisticated groups routinely exploit vulnerabilities in Windows environments, capitalizing on unpatched vulnerabilities, leaving organizations exposed to cyber threats. The most critical defense in maintaining the security of Windows system is patch management.

Overview of Research

The Importance of Patch Management

The most critical aspect of Windows cybersecurity is effective patch management. According to Dissanayake et Al (2020) patch management refers to the process of applying patches to the vulnerabilities present in software products and systems in IT environments. Patching is not just a routine IT task to complete; it is a proactive security measure that requires detailed planning, risk assessments, several tests, deployment tactics, and verification. Research has shown that the majority of successful cyberattacks target patch vulnerabilities that already existed at the time of exploitation (Dissanayake et al., 2020).

Patch Management Failures

The well-known WannaCry ransomware attack in 2017 is a perfect example of existing vulnerabilities leading up to a cyber attack. However, Microsoft released a patch for the SMBv1 vulnerability months prior to, in which thousands of organizations failed to apply it immediately, which resulted in the widespread compromise across global healthcare, finance, and government sectors (Darzi et al., 2019). A similar situation occurred again with the PrintNightmare series of vulnerabilities in 2021, where delays, uncertainties, and incomplete patch deployments increased the risk of remote code attacks within Windows Print Spooler services. Regardless of the availability of advanced management tools such as Windows Server Update Services (WSUS), Microsoft Intune, and System Center Configuration Manager (SCCM), many organizations and industries continue to struggle with carrying out timely and consistent patch cycles. This is most likely due to operational constraints, dependencies on systems, fear of inactive periods of time, resource limitations, and insufficient frameworks. As Dissanayake (2022) observed in a study in the healthcare sector, even severely high vulnerabilities may go unpatched when administrators believe that updates could interrupt critical services. These challenges highlight the tension between system stability and security, which remains at the core of Windows management best practices.

Frameworks

NIST SP 800-40 outlines best practices that organizations should adopt to strengthen patch management. Scarfone and Souppaya (2021) emphasize asset inventory tracking, patch identification, risk prioritization, controlled testing, phased deployments, and full verification. Zero Trust architecture complements patch management by requiring continuous compliance before granting access to systems. Sharma and Gupta (2020) argue that Zero Trust reduces the

likelihood that unpatched devices can be used for lateral movement. Tools, Resources, and Results Windows Update, WSUS, SCCM, and Intune are central components of Microsoft's patching ecosystem. Enterprises benefit from using automation to reduce delays. Dissanayake et al. (2020) found that automated patch cycles reduced remediation times by up to 60%. Hafiz and Adam (2022) highlight that patching and privilege management are highly effective defenses against ransomware.

Windows security requires more than patching alone. Microsoft's evolving architecture emphasizes a layered security model that incorporates identity protection, endpoint hardening, encrypted communication, and Zero Trust principles. Tools such as Microsoft Defender, Credential Guard, BitLocker, and Windows Firewall supplement patch management by reducing attack surfaces and limiting adversary movement. However, the effectiveness of these tools depends heavily on how organizations configure, monitor, and enforce them. Without clear processes and well-structured frameworks, even most advanced security features can fail to protect against modern threats. For these reasons, Windows management and cybersecurity are inseparable elements of enterprise risk reduction. Effective management requires not only tools and technology, but also policies, training, governance, and continuous monitoring. To fully understand Windows cybersecurity today, organizations must examine not just the threats and vulnerabilities, but also the frameworks, processes, and methodologies that support secure Windows operations.

The research on Windows management and cybersecurity consistently emphasizes that effective system protection requires a comprehensive understanding of both the technical vulnerabilities within Windows environments and the organizational factors that influence patching and security practices. Because attackers often weaponize newly disclosed

vulnerabilities within days, organizations must rely on structured frameworks, such as NIST SP 800-40 and Microsoft's security baselines, to guide their update policies, testing procedures, and deployment workflows. Additionally, the literature underscores the importance of complementary defenses, such as Zero Trust principles, privilege management, and endpoint protection tools like Microsoft Defender and Credential Guard, all of which reinforce patching by reducing attack surfaces. Together, these studies demonstrate that securing Windows environments requires not only timely updates but also a well-governed, multi-layered cybersecurity approach supported by research-informed best practices.

Tools

Without structured processes, Windows systems accumulate vulnerabilities that attackers can exploit rapidly, sometimes within days of public disclosure. Research and Required Information Patch management is a proactive measure that addresses vulnerabilities before adversaries can exploit

Windows systems face a wide range of vulnerability types, including remote code execution (RCE), privilege escalation, memory corruption, and credential theft vulnerabilities. Romanosky (2019) emphasizes that attackers often weaponize new vulnerabilities within weeks of disclosure, creating a critical "window of exposure." Case Study Analysis WannaCry exploited the SMBv1 vulnerability MS17-010, despite Microsoft releasing a patch months earlier. Darzi et al. (2019) found that approximately one-third of NHS England facilities were directly affected. PrintNightmare (2021) demonstrated the complications of patching Windows Print Spooler vulnerabilities. Jenkins et al. (2023) found that system administrators often lacked clarity about which patches were complete and safe to deploy.

A primary tool that organizations use to manage Windows vulnerabilities is Patch Tuesday; this event occurs on a monthly basis and during each event, Microsoft distributes security patches for its software products. As a result of the periodic nature of the patch process, organizations can maintain a position of being ahead of the curve when it comes to the threat posed by potential cyber threats as these are resolved prior to an attacker exploiting the identified vulnerability. These regular updates provide essential protection to mitigate risk related to many types of vulnerabilities including remote code execution, privilege escalation and information disclosure. The following table from Microsoft (2025) provides examples of significant vulnerabilities resolved through November 2025 most recent Patch Tuesdays. Listed in the table is the CVE ID, the Patch (MS Bulletin ID) and the CVSS Base Score. The CVE ID identifies each vulnerability, the Patch (MS Bulletin ID) refers to the official patch release form Microsoft, and the CVSS Base Score measures the severity of the vulnerability. CVSS base scores of 8.0 or higher, represent critical risks that require immediate attention.

Vulnerability (CVE ID)	Patch (MS Bulletin ID)	CVSS Base Score
CVE-2025-60716	KB5068861, KB5068966	7.0
CVE-2025-60717	KB5068791	7.0
CVE-2025-60724	KB5068864	9.8
CVE-2025-62208	KB5066836	5.5
CVE-2025-62213	KB5068905	7.0
CVE-2025-62459	(Pending / To be released)	8.2

This demonstrates why timely updates are necessary to limit an organization's exposure to cyber attacks. By regularly complying with Patch Tuesday, organizations can mitigate risks and reduce the likelihood of exploitation.

Conclusion

Challenges remain, including human hesitation, compatibility concerns, resource shortages, and the presence of legacy systems. Still, organizations that adopt structured patch cycles experience significantly fewer incidents. Patch management is one of the most important components of Windows cybersecurity. Timely patching reduces exposure to known vulnerabilities and prevents attackers from exploiting high-risk flaws. Frameworks such as NIST SP 800-40 and architectures such as Zero Trust provide structure and enhance enforcement. Ultimately, effective patch management requires automation, governance, and a culture of continuous improvement.

References

Dissanayake, N., Jayatilaka, A., Zahedi, M., & Babar, M. A. (2020). Software security patch management: A systematic literature review of challenges, approaches, tools and practices. arXiv. https://arxiv.org/abs/2012.00544

Dissanayake, N., Jayatilaka, A., Zahedi, M., & Babar, M. A. (2022). Why, how and where of delays in software security patch management: An empirical investigation in the healthcare sector. arXiv. https://arxiv.org/abs/2202.09016

Darzi, A., Archer, S., Chen, R., Black, G., Majeed, A., & Huckvale, K. (2019). A retrospective impact analysis of the WannaCry cyberattack on the NHS in England. NPJ Digital Medicine, 2(1), 98. https://doi.org/10.1038/s41746-019-0161-6

Jenkins, A., Wolters, M., & Vaniea, K. (2023). To patch, or not to patch? That is the question: A case study of system administrators' online collaborative behaviour. arXiv. https://arxiv.org/abs/2307.03609

Microsoft. (2025). Security Update Guide - Microsoft Security Response Center. Msrc.microsoft.com. https://msrc.microsoft.com/update-guide/

Bhalla, P. (2025, October 13). Windows Statistics By Market Share, Trends, Insights And Facts (2025). Electro IQ. https://electroiq.com/stats/windows-statistics/

Scarfone, K., & Souppaya, M. (2021). Guide to enterprise patch management planning (NIST SP 800-40 Revision 4). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-40r4

Sharma, A., & Gupta, R. (2020). Zero Trust implementation for Windows enterprise systems. Journal of Cybersecurity, 6(1), 1–15.

https://msrc.microsoft.com/update-guide/