Windows System Security Vulnerabilities

Jonathan Roeseler

Old Dominion University

CYSE 280

July 31, 2025

Windows, an OS developed by Microsoft, is the premier operating system on the market for both civilian and enterprise use, with some estimates placing it on seventy percent of desktops (“Operating System”). With great power comes great responsibility, and when it comes to Microsoft and the Windows platform, they shift the burden onto the end-user to manage and figure their systems out (!). Microsoft’s products and environments, including Active Directory, are plagued by insecure default configurations, insecure design, and misconfiguration(s). According to a paper by Mr. Softić and Vejzović, Windows is found to have the most severe vulnerabilities compared to the other most commonly used operating systems. This paper will introduce the basic design of Windows and Active Directory, then lay out some common issues/misconfigurations, vulnerabilities (including those where it's Microsoft's fault), before finally offering how to mitigate some of the shown issues. Microsoft’s products are attacked every day, and every year, it seems like something of theirs is largely taken advantage of, resulting in widespread breaches or impact. The paper intends to enhance the security of these products for end-users.

Microsoft offers many products, but most notably is Active Directory [AD], which is used by most enterprise and government institutions to manage and secure their networks, devices, and users. One of the most common ways to secure and manage devices in an AD environment is through Administrative Templates and Group Policy Objects [GPO] (Allen and Lowe-Norris). Even with these properly configured and solid baselines set to secure your environment through these policies, attackers can still easily find their way in - and sometimes it's not even your fault! Microsoft is known for its vulnerable products - a great example being the Eternal Blue vulnerability. This vulnerability was used in one of the most notorious hacking campaigns ever seen - WannaCry. In this attack, actors exploited a vulnerability in Windows’

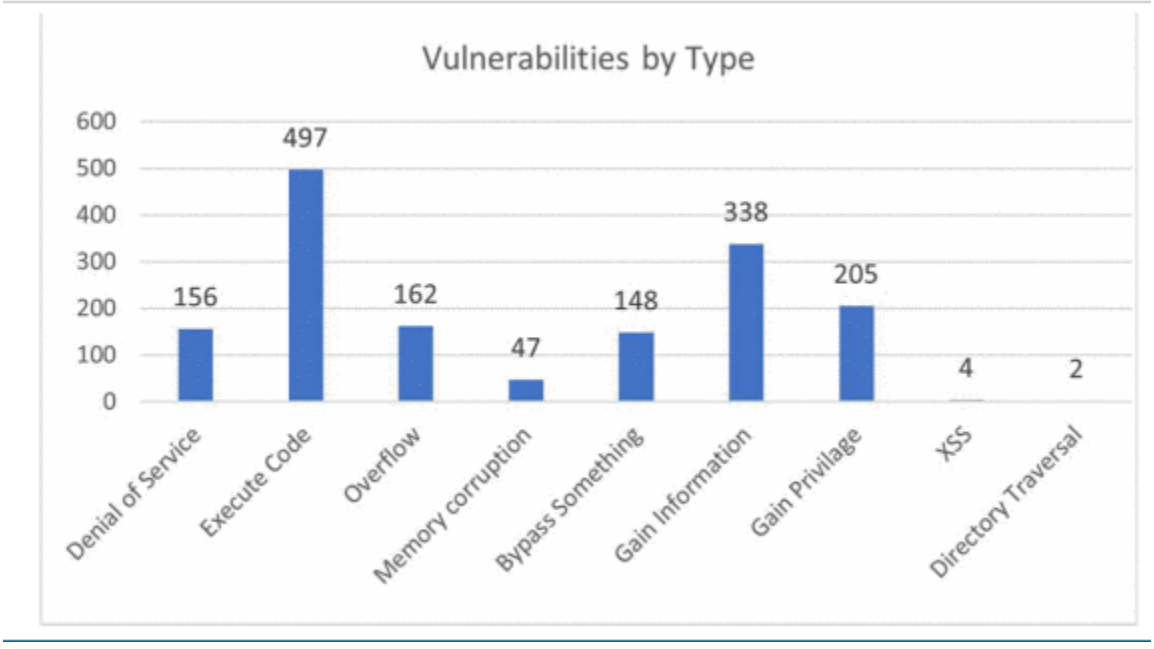
own protocol, Server Message Block [SMB], which is used for file and printer sharing, to exploit hundreds of thousands of devices across the globe (Gupta). The attacker did not even require authentication for this vulnerability; all that was needed to be done was to send a specially crafted packet to the vulnerable device, and you were then essentially the root or owner of the device. Interestingly, despite being one of the most infamous computer attacks, many (thousands) of devices are still vulnerable to this exploit. You can try this yourself by going to shodan.io and searching for the vulnerability (ms17-010). MS17-010 or Eternal Blue is a great example of the need for patching/updating definitions to prevent attacks, as this exploit would again show up later in other infamous ransomware campaigns (NotPetya). History tends to repeat or echo itself, and today (July 23). Microsoft is experiencing similar pains, this time with another zero-day on its SharePoint service. This impacted all organizations utilizing an on-prem SharePoint server(s) (Goodin). Once again, Microsoft is at fault, and even after systems around the world were getting compromised, it took days to release a patch. Interestingly, their advice at the time was to completely take down the server as there was no other solution to mitigate it. Moving on from Microsoft's design failures, another common vector of attack is finding misconfigurations of Microsoft systems. Some common ones include: Administrative privilege (usually too many or configured incorrectly), weak passwords and/or password policy (such as not enforcing strong passwords or MFA), and legacy/unpatched systems (Smith). All of these can be corrected, which is why it's essential to determine your security posture through scans from third-party vendors, such as CrowdStrike, or automated tools that can find these misconfigurations. Microsoft does have a suite of tools to identify misconfigurations and vulnerabilities in its environment. As Microsoft moves to the cloud with many offerings, it has developed many additional tools to secure these complex environments. Some of the common

tools include Defender (for Endpoint, Cloud, 365), Intune (Device management), Sentinel (Microsoft's SIEM solution), and Entra for identity protection (Rise and Engen). Despite these additional offerings, many organizations still struggle to secure their environments. Even if moving to a solely cloud environment, vulnerabilities still largely exist, even with the underlying hardware and OS update/patching not being in the user's/organization's control or their responsibility. Microsoft changes and adds features all the time, which can open organizations using their services, especially in the cloud, to attacks. A good example of this is their direct-send feature in Exchange (email solution). Usually, when in an on-premises environment, this is not really an issue as it is managed internally. However, in the cloud, attackers can bypass third-party security solutions and impersonate internal users very easily with this feature, leading to Microsoft having to introduce an option to turn it off entirely (Barnea). Windows can be a secure OS; however, it takes both a responsible administrator and competent development and research by Microsoft itself to ensure its safety.

There are many ways to evaluate a Windows system's security and configuration. In fact, many businesses make a living off of scanning Windows environments for their customers and displaying results. An example of this would be something like "this GPO should be configured to ensure this privilege escalation technique cannot take place". Some common examples of tools to identify and ensure secure baselines include: DOD STIGs, Microsoft's Security Compliance Toolkit, and SCAP tools (Stöckle, et al.). It is important to note that Microsoft has many products, so these tools do not work in an environment that is entirely cloud-based (SaaS) or using a service such as Intune for policy enforcement and/or device management instead of Active Directory. Such use-cases require their own benchmarks and secure configurations; however, these tools are not readily available from Microsoft and usually require special vendors

to scan these cloud environments(SaaS/PaaS) like those primarily working on/through Microsoft Intune and/or SharePoint. In the scans below, results will be compared against Microsoft's recommended settings and baselines; however, every implementation is different, and it's necessary to understand your environment before choosing a framework and its respective tooling to secure your environment.

While there are many tools able to identify and scan for vulnerabilities, for this research, only Metasploit, Nessus, and Nmap will be used. These tools will give the best illustration of what it looks like externally to a curious attacker. As the security environment across the globe continues to develop, attackers are also becoming increasingly sophisticated. With that being said, Microsoft systems tend to introduce new vulnerabilities over the years. Here are the most common vulnerability types in Windows systems.



This chart shows the vulnerabilities found in the Windows 10 OS (Softić and Vejzović). Of the scans run, externally, most Windows OS are secure, as long as they are updated. The most

common cause of breach is user error, such as clicking a link or downloading a file from a phishing email. Windows can be very secure systems if managed correctly; however, when Microsoft's protocols or design flaws are exposed, it opens up those systems to exploitation, as seen with EternalBlue or the current SharePoint attack mentioned previously. Keeping systems up-to-date and applying Microsoft's secure baselines mitigates almost all types of attack. It usually takes a sophisticated actor with a chain of complex exploits in a secure system to elevate permissions and cause serious damage to an AD or Windows system/environment.

Windows systems, especially in enterprise scenarios, are a complex OS to manage and keep secure. Despite this, there are many tools to remediate and apply a strong and secure baseline to every device needed (server or desktop). Some of the strongest methods to keep these systems secure are to regularly update and patch, move to systems that are not at End-Of-Service or End-Of-Life, and manage GPOs or other policies depending on the Microsoft environment with security in mind. Continuous monitoring and configuration audits are vital to identify gaps and adjust security posture as threats evolve. User and administrative training are essential to further strengthen a Windows environment, as human error is still the leading cause of breach.

References

Allen, Robbie, and Alistair Lowe-Norris. *Active directory*. " O'Reilly Media, Inc.", 2003.

Barnea, Tom. “Ongoing Campaign Abuses Microsoft 365’s Direct Send to Deliver Phishing Emails.” *Varonis*, Varonis, 27 June 2025, www.varonis.com/blog/direct-send-exploit.

Goodin, Dan. “SharePoint Vulnerability with 9.8 Severity Rating under Exploit across Globe.” *Ars Technica*, 21 July 2025, arstechnica.com/security/2025/07/sharepoint-vulnerability-with-9-8-severity-rating-is-under-exploit-across-the-globe/.

Gupta, Manoj R., et al. "Eternal blue vulnerability." *International Journal for Research in Applied Science & Engineering Technology (IJRASET)* 11.6 (2023): 1054.

J. Softić and Z. Vejzović, "Windows 10 Operating System: Vulnerability Assessment and Exploitation," 2022 21st International Symposium INFOTEH-JAHORINA (INFOTEH), East Sarajevo, Bosnia and Herzegovina, 2022, pp. 1-5, doi: 10.1109/INFOTEH53737.2022.9751274.

“Operating System/Windows Share (End of January 2025).” *Borns Tech and Windows World*, borncity.com/win/2025/02/03/operating-system-windows-share-end-of-january-2025/. Accessed 23 July 2025.

Rise, Helleik Rabba, and Stian Engen. *Windows Server 2019/2022 and Azure Cloud security systems-A general recommendation*. BS thesis. NTNU, 2022.

Smith, Peyton. “Skeletons in the IT Closet: Seven Common Microsoft Active Directory Misconfigurations That Adversaries Abuse.” *CrowdStrike*, www.crowdstrike.com/en-us/blog/seven-common-microsoft-ad-misconfigurations-that-adversaries-abuse/. Accessed 23 July 2025.

Stöckle, Patrick, Bernd Grobauer, and Alexander Pretschner. "Automated implementation of windows-related security-configuration guides." *Proceedings of the 35th IEEE/ACM International Conference on Automated Software Engineering*. 2020.