**Legacy Operating Systems**

While this module primarily focuses on modern operating systems (Windows 10/Windows Server 2016), as we have seen, certain issues (i.e., vulnerable software, misconfigurations, careless users, etc.) cannot be solved by merely upgrading to the latest and greatest Windows desktop and server versions. That being said, specific security improvements have been made over the years that no longer affect modern, supported versions of the Windows operating system. During our assessments, we will undoubtedly encounter legacy operating systems (especially against large organizations such as universities, hospitals/medical organizations, insurance companies, utilities, state/local government). It is essential to understand the differences and certain additional flaws that we need to check to ensure our assessments are as thorough as possible.

**End of Life Systems (EOL)**

Over time, Microsoft decides to no longer offer ongoing support for specific operating system versions. When they stop supporting a version of Windows, they stop releasing security updates for the version in question. Windows systems first go into an "extended support" period before being classified as end-of-life or no longer officially supported. Microsoft continues to create security updates for these systems offered to large organizations through custom long-term support contracts. Below is a list of popular Windows versions and their end of life dates:

**Windows Desktop - EOL Dates by Version**

| **Version** | **Date** |
| --- | --- |
| Windows XP | April 8, 2014 |
| Windows Vista | April 11, 2017 |
| Windows 7 | January 14, 2020 |
| Windows 8 | January 12, 2016 |
| Windows 8.1 | January 10, 2023 |
| Windows 10 release 1507 | May 9, 2017 |
| Windows 10 release 1703 | October 9, 2018 |
| Windows 10 release 1809 | November 10, 2020 |
| Windows 10 release 1903 | December 8, 2020 |
| Windows 10 release 1909 | May 11, 2021 |
| Windows 10 release 2004 | December 14, 2021 |
| Windows 10 release 20H2 | May 10, 2022 |

**Windows Server - EOL Dates by Version**

| **Version** | **Date** |
| --- | --- |
| Windows Server 2003 | April 8, 2014 |
| Windows Server 2003 R2 | July 14, 2015 |
| Windows Server 2008 | January 14, 2020 |
| Windows Server 2008 R2 | January 14, 2020 |
| Windows Server 2012 | October 10, 2023 |
| Windows Server 2012 R2 | October 10, 2023 |
| Windows Server 2016 | January 12, 2027 |
| Windows Server 2019 | January 9, 2029 |

This [page](https://michaelspice.net/windows/end-of-life-microsoft-windows-and-office/) has a more detailed listing of the end-of-life dates for Microsoft Windows and other products such as Exchange, SQL Server, and Microsoft Office, all of which we may run into during our assessments.

**Impact**

When operating systems are set to end of life and are no longer officially supported, there are many issues that may present themselves:

| **Issue** | **Description** |
| --- | --- |
| Lack of support from software companies | Certain applications (such as web browsers and other essential applications) may cease to work once a version of Windows is no longer officially supported. |
| Hardware issues | Newer hardware components will likely stop working on legacy systems. |
| Security flaws | This is the big one with a few notable exceptions (such as [CVE-2020-1350](https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-1350) (SIGRed) or EternalBlue ([CVE-2017-0144](https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2017-0144))) which were easily exploitable and "wormable" security flaws which affected thousands of systems worldwide (including critical infrastructure such as hospitals). Microsoft will no longer release security updates for end-of-life systems. This could leave the systems open to remote code execution and privilege escalation flaws that will remain unpatched until the system is upgraded or retired. |

In some instances, it is difficult or impossible for an organization to upgrade or retire an end-of-life system due to cost and personnel constraints. The system may be running mission-critical software no longer supported by the original vendor. This is common in medical settings and local government, where the vendor for a critical application goes out of business or no longer provides support for an application, so the organization is stuck running it on a version of Windows XP or even Server 2000/2003. If we discover this during an assessment, it is best to discuss with the client to understand the business reasons why they cannot upgrade or retire the system(s) and suggest solutions such as strict network segmentation to isolate these systems until they can be dealt with appropriately.

As penetration testers, we will often come across legacy operating systems. Though I do not see many hosts running server 2000 or Windows XP workstations vulnerable to [MS08-067](https://docs.microsoft.com/en-us/security-updates/securitybulletins/2008/ms08-067), they exist, and I come across them on occasion. It is more common to see a few Server 2003 hosts and 2008 hosts. When we come across these systems, they are often vulnerable to one or multiple remote code execution flaws or local privilege escalation vectors. They can be a great foothold into the environment. However, when attacking them, we should always check with the client to ensure they are not fragile hosts running mission-critical applications that could cause a massive outage. There are several security protections in newer Windows operating system versions that do not exist in legacy versions, making our privilege escalation tasks much more straightforward.

There are some notable differences among older and newer versions of Windows operating system versions. While this module aims to teach local privilege escalation techniques that can be used against modern Windows OS versions, we would be remiss in not going over some of the key differences between the most common versions. The core of the module focuses on various versions of Windows 10, Server 2016, and 2019, but let's take a trip down memory lane and analyze both a Windows 7 and a Server 2008 system from the perspective of a penetration tester with the goal of picking out key differences that are crucial during assessments of large environments.