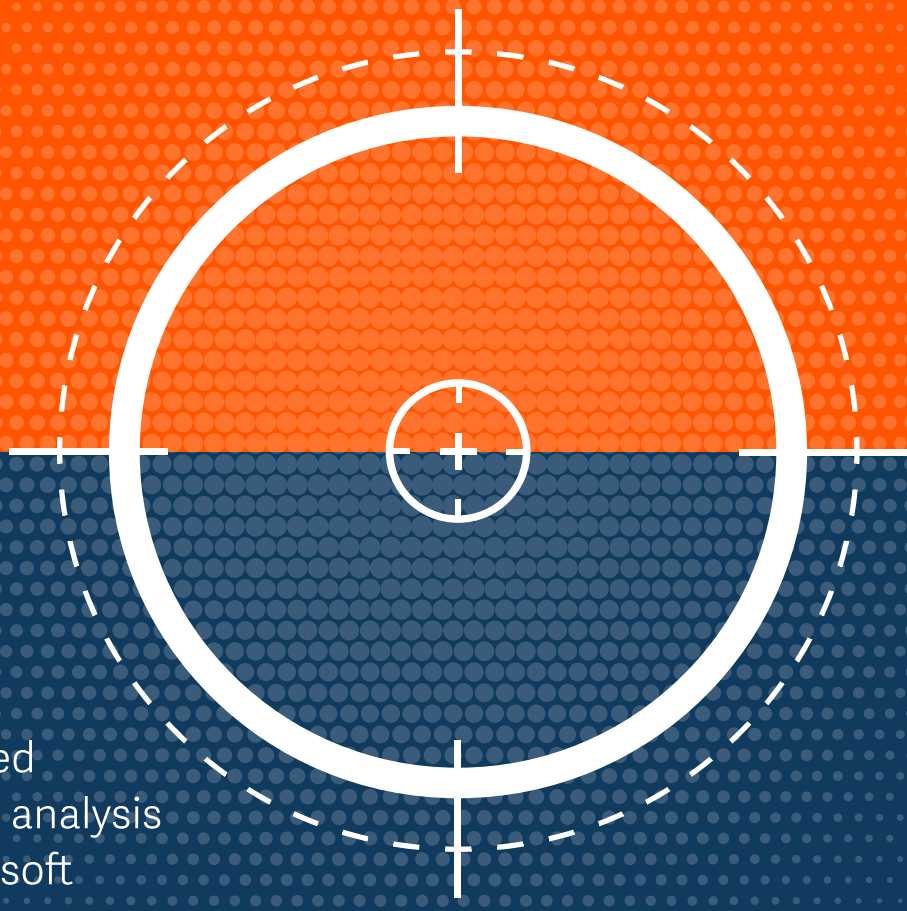
BeyondTrust

Are organizations having an identity crisis?

2024 Microsoft Vulnerabilities Report



Benefit from research-backed insights and industry expert analysis to better protect your Microsoft estate in 2024 and beyond

BeyondTrust

TABLE OF CONTENTS

Executive Summary

Following our 10th anniversary edition, this year we are ***turning things up to 11*** by asking one key question as we look across the Microsoft vulnerability landscape:

"Are organizations having an identity crisis?"

Through its 11 years in publication, the Microsoft Vulnerabilities Report has garnered over 16,000 downloads and helped thousands of users leverage its detailed data analysis and expert findings to improve their cyber defenses.

This year's edition of the report not only dissects the 2023 Microsoft vulnerabilities data, but also assesses how these vulnerabilities are being leveraged in identity-based attacks. The report also spotlights some of the most significant CVEs of 2023 (9.0+ CVSS severity scores), breaks down how they are leveraged by attackers, and explains how they can be mitigated.

A panel of some of the world's leading cybersecurity experts will weigh in on the report findings as we collectively set our sights forward on emerging threats, new vulnerabilities, and how to best build cyber resilience across the enterprise and society at large.

Read on to better understand, identify, and address the risks facing your organization within the Microsoft ecosystem.

Key Findings & Data Highlights

Key Findings

After hitting an all-time high in the number of reported Microsoft vulnerabilities in 2022, total reported vulnerabilities have slightly receded.

Looking at the larger trend, the number of Microsoft vulnerabilities has plateaued since 2020.

Total vulnerabilities continue their 4-year holding pattern near their highest-ever numbers. While dropping slightly (by 5%) from 1,292 to 1,228 in 2023, total vulnerabilities have held firm near their all-time highs, remaining between 1,200 and 1,300 for the past four years (since 2020).

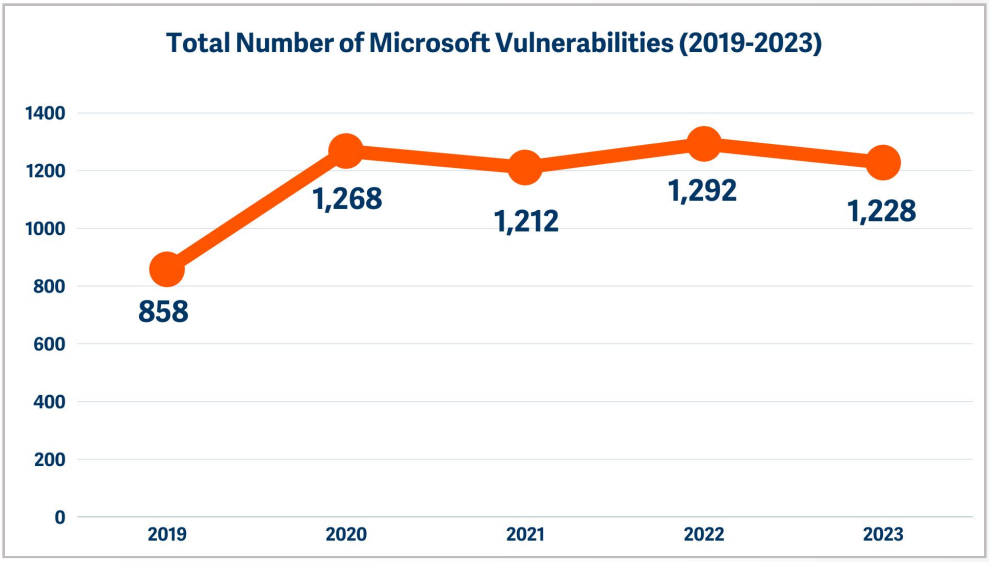
Elevation of Privilege vulnerability category continues to dominate. Continuing the trend in post-pandemic years, Elevation of Privilege accounted for 40% (490) of the total vulnerabilities in 2023.

The total number of critical vulnerabilities continues its downward trend, but slowly. Critical vulnerabilities dropped by 6% to 84 in 2023 (5 less than 2022).

Data Highlights

- After Microsoft Azure & Dynamics 365 vulnerabilities skyrocketed in 2022, they almost halved in 2023 – down from 114 to 63.
- Microsoft Edge experienced 249 vulnerabilities in 2023, only one of which was critical.
- There were 522 Windows vulnerabilities in 2023, 55 of which were critical.
- Microsoft Office experienced 62 vulnerabilities in 2023.
- Windows Server category had 558 vulnerabilities in 2023, 57 of which were critical.
- Denial of Service vulnerabilities climbed 51% to hit a record high of 109 in 2023, with Spoofing demonstrating a dramatic 190% increase, from 31 to 90.

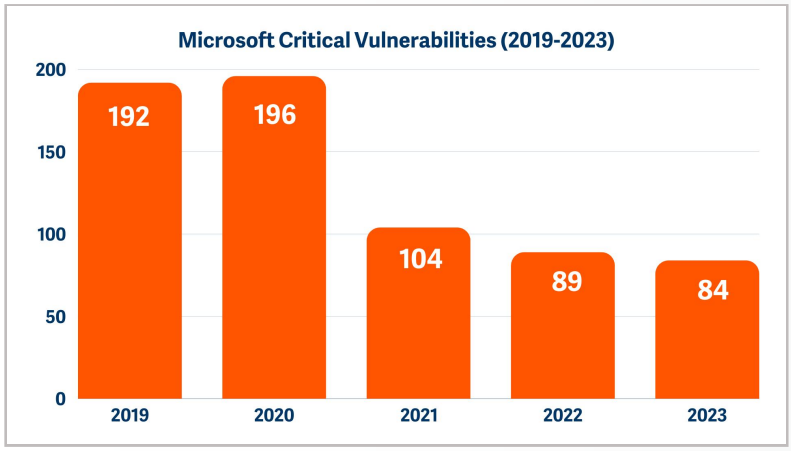
5-Year Trend



Total number of vulnerabilities have plateaued, remaining between 1,200 and 1,300 for the past four years.

Following the dramatic increase of Microsoft vulnerabilities in 2020, we have observed the total number of vulnerabilities plateauing over the past four years, with the range of fluctuations staying within a 7% window.

Total vulnerabilities hit 1,228 in 2023, which represents a 5% decrease over the previous year, after hitting an all-time-high of 1,292 in 2022.

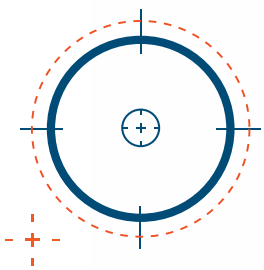


Critical vulnerabilities continued their downward trend in 2023, but the pace has slowed.

Similarly, critical vulnerabilities have remained steady, dipping slightly from 89 in 2022 to 84 in 2023. In terms of both total and critical vulnerabilities, this makes the past two years some of the most consistent we have seen since this report's debut eleven years ago, with no major swings in the core data.

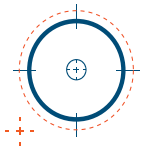
Looking at the distribution of critical vulnerabilities year over year, we observe a consistent downward trend. Windows Desktop and Server categories have both remained the main source of critical vulnerabilities through 2023. Given that they share a similar codebase, which represents a progressive evolution of the Windows NT Kernel, this is not a surprise.

As we discussed in last year's report, there are areas of Windows operating systems with ~20-year-old, often long-forgotten code that can come back to haunt us—even on the latest versions of Windows. Over time, these risks have been steadily decreasing as the longtail of services and features have been refreshed. This plays a part in why we are seeing stability in the data today, which we will cover in greater depth below.



A major source of risk for organizations everywhere, critical vulnerabilities, when exploited, have the potential to result in high-impact security events. These are the vulnerabilities that keep IT admins awake at night.

What does stable vulnerabilities data tell us?



Stable vulnerabilities data is a strong indicator that overall long-term security efforts are paying off.

As we discussed in previous reports, an absence of sharp increases, as well as consistently decreasing numbers, are good indicators that many of Microsoft's longer-term security efforts are paying off.

Legacy products, many of which were first developed before Microsoft introduced their Security Development Lifecycle in 2004, have come to End-of-Life (EOL), and newer, more secure operating systems and products have taken their place. Cloud technologies have matured, and those security investments have paid off.

Even looking back just three years, we see a starkly different picture. In 2020, critical vulnerability numbers were 133% higher than they were in 2023. While this year's data hasn't revealed as big a decrease in critical vulnerabilities as it has in previous years, the steady downward trend continues. This is a reassuring finding—especially for the IT practitioners who live and breathe the security of their Microsoft systems.

Understanding Microsoft Critical Vulnerabilities

The total number of vulnerabilities are an important indicator of an environment's health, but vulnerabilities are not created equal.

Some vulnerabilities may pose mostly theoretical risk (low likelihood and low impact) if they are exploited. On the opposite side of the spectrum, other vulnerabilities have high likelihoods of exploitation, and their exploitation may result in a highly negative impact to the affected organization(s).

Measuring a vulnerability's level of impact relates to its impact on the confidentiality, integrity, and availability of data within a system or organization. The most severe vulnerabilities will impact all three of these basic tenets of information security.

Vulnerabilities categorized as 'critical' are those with characteristics that make their exploitation a potentially high-impact security event. The way Microsoft classifies the severity rating for a vulnerability is distinct from the likelihood of exploitation.

However, the likelihood of exploitation is far more dynamic because attackers are more likely to exploit a known vulnerability.

Exploitation of 'critical' vulnerabilities will:

Likely result in total compromise of a device or infrastructure.

Have fewer prerequisites. Usually, the attack would not require any special access, privileges, or advanced knowledge.

Allow code execution without user interaction. These generally do not rely on social engineering.

These types of vulnerabilities are what keep IT admins awake at night and are a major source of risk organizations everywhere must contend with.

How does Microsoft classify critical vulnerabilities?

The National Vulnerabilities Database (NVD) classifies critical vulnerabilities as those awarded a Common Vulnerability Scoring System (CVSS) score of 9.0-10.0. The more enthusiastic readers of Microsoft's vulnerability announcements may have noticed that, while Microsoft now uses CVSS 3.1 scoring for their vulnerabilities, they rank severities based on Microsoft's own Security Update Severity Rating System. This rates each vulnerability according to the worst theoretical outcome should that vulnerability be exploited.

This means that:

While 33 Microsoft vulnerabilities from 2023 scored a 9.0 or above (a 50% increase from 22 in 2022), making them "critical" under the National Vulnerability Database scoring system, Microsoft has classified 84 of its vulnerabilities as critical in 2023 (down 6% from 89 in 2022).

CVSS 3.1 Ratings

Severity	Base Score Range
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

Fig. 1: The National Vulnerabilities Database (NVD) scoring system for classifying critical vulnerabilities

Microsoft Security Update Rating System | Rating & Description

Critical
A vulnerability whose exploitation could allow code execution without user interaction. These scenarios include self-propagating malware (e.g. network worms), or avoidable common use scenarios where code execution occurs without warnings or prompts. This could mean browsing to a web page or opening email. Microsoft recommends that customers apply critical updates immediately.

Important
A vulnerability whose exploitation could result in compromise of the confidentiality, integrity, or availability of user data, or of the integrity or availability of processing resources. These scenarios include common use scenarios where a client is compromised with warnings or prompts regardless of the prompt's provenance, quality, or usability. Sequences of user actions that do not generate prompts or warnings are also covered. Microsoft recommends that customers apply important updates at the earliest opportunity.

Moderate
Impact of the vulnerability is mitigated to a significant degree by factors such as authentication requirements or applicability only to non-default configurations. Microsoft recommends that customers consider applying the security update.

Low
Impact of the vulnerability is comprehensively mitigated by the characteristics of the affected component. Microsoft recommends that customers evaluate whether to apply the security update to the affected systems.

Fig 2: The Microsoft Security Update Severity Rating System for identifying associated risk based on the worst theoretical outcome, if that vulnerability were to be exploited

The difference between CVSS scoring and Microsoft's severity rating system is worth noting, not only when considering the data in this report, but also when considering risk in your organization.

CVSS scores measure the technical severity of a vulnerability (i.e. whether a vulnerability results in some loss of data confidentiality or total loss of confidentiality). CVSS scoring does not measure the risk of that vulnerability. This means CVSS scores alone cannot tell you whether a vulnerability will cause a mission-critical impact on a system, or if the limited loss of some highly sensitive data would have a more severe impact than the total loss of non-sensitive data.

Microsoft's severity rating system is potentially far more useful than a base or temporal CVSS score for security practitioners trying to prioritize risk reduction. However, it is important to know your own environment and risks so you can understand how best to prioritize patches and/or use other security hardening controls and mitigations.

All the data provided by Microsoft's severity rating system is based on the information available at the time. It lacks the context of your own organization's threat models. What is considered a critical patch for one organization may not be so for another organization—it all depends on the business context.

In addition to their Security Update Severity Rating System, Microsoft has also published an Exploitability Index to help customers understand the likelihood of exploitation. This can be useful information for those needing help with prioritization of security updates. As a word of caution, this information reflects the likelihood of exploitation at the time the security update was published. It may not reflect the real-world exploitability that develops in the following weeks or months as more threat actors weaponize the vulnerability. The index is best used for very short-term prioritization of updates, rather than as a justification to significantly delay patching.

Microsoft Exploitability Index

Fig. 3: The Microsoft Exploitability Index for assessing the likelihood of exploitation at the time the security update was published

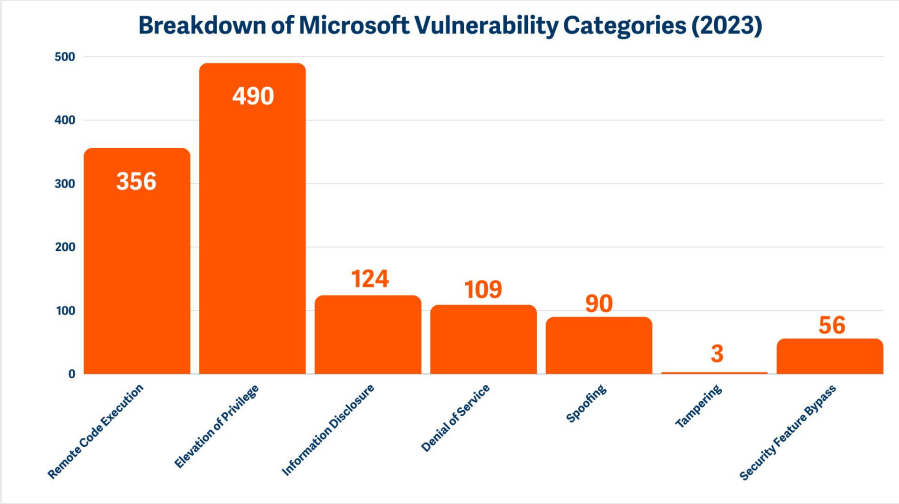
Index	Short Definition	Expanded Definition
0	Exploitation Detected	Microsoft is aware of an instance of this vulnerability being exploited. As such, customers who have reviewed the security update and determined its applicability within their environment should treat this with the highest priority.
1	Exploitation More Likely	Microsoft analysis has shown that exploit code could be created in such a way that an attacker could consistently exploit this vulnerability. Moreover, Microsoft is aware of past instances of this type of vulnerability being exploited. This would make it an attractive target for attackers, and therefore, more likely that exploits could be created. As such, customers who have reviewed the security update and determined its applicability within their environment should treat this with a higher priority.
2	Exploitation Less Likely	Microsoft analysis has shown that while exploit code could be created, an attacker would likely have difficulty creating the code, requiring expertise and/or sophisticated timing, and/or varied results when targeting the affected product. Moreover, Microsoft has not recently observed a trend of this type of vulnerability being actively exploited in the wild. This makes it a less attractive target for attackers. That said, customers who reviewed the security update and determined its applicability within their environment should still treat this as a material update. If they are prioritizing against other highly exploitable vulnerabilities, they could rank this lower in their deployment priority.
3	Exploitation Unlikely	Microsoft analysis shows that successfully functioning exploit code is unlikely to be utilized in real attacks. This means that while it might be possible for exploit code to be release that could trigger the vulnerability and cause abnormal behavior, the full impact of exploitation will be more limited. Moreover, Microsoft has not observed instances of this type of vulnerability being actively exploited in the past. Thus, the actual risk of being exploited from the vulnerability is significantly lower. Therefore, customers who have reviewed the security update to determine its applicability within their environment could prioritize this update below other vulnerabilities within a release.

Vulnerabilities Data Deep Dive

Vulnerabilities by Category

Each Microsoft Security Bulletin is comprised of one or more vulnerabilities, which apply to one or more Microsoft products.

Microsoft typically groups vulnerabilities into these main categories:
Remote Code Execution (RCE), Elevation of Privilege (EoP), Information Disclosure, Denial of Service (DDoS), Spoofing, Tampering, and Security Feature Bypass.



Elevation of Privilege remains the #1 vulnerability category, despite a significant 31% drop from 715 to 490 over the previous year.

Microsoft Vulnerability Categories (2019-2023)

	2019	2020	2021	2022	2023
Remote Code Execution	323	345	326	314	356
Elevation of Privilege	198	559	588	715	490
Information Disclosure	177	179	129	114	124
Denial of Service	52	46	55	72	109
Spoofing	63	104	66	31	90
Tampering	8	7	3	4	3
Security Feature Bypass	38	30	44	42	56

Remote Code Execution breaks its downward trend in 2023, increasing by 13% to 356, the highest number we've seen since this report's debut.

Remote Code Execution and Elevation of Privilege remain the top vulnerability categories, once again highlighting familiar threat actor objectives.

Elevation of Privilege remains the #1 vulnerability category in 2023

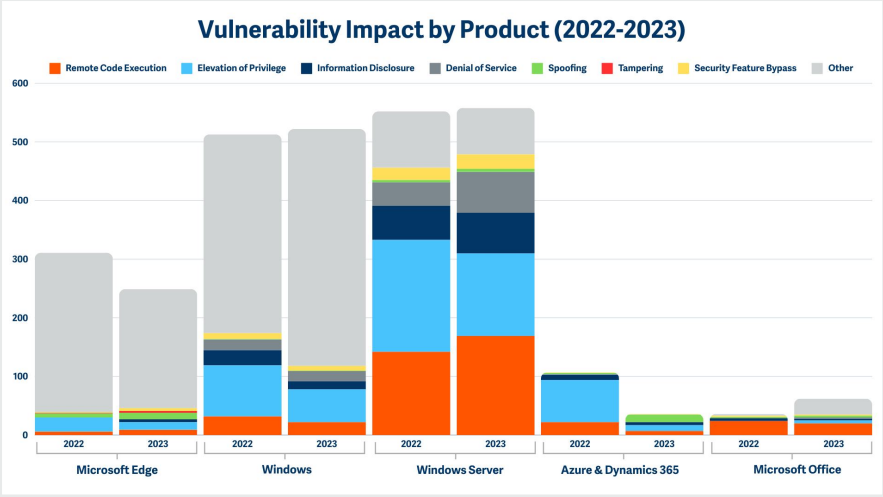
Elevation of Privilege has continued its post-2019 trend and remains the #1 category of vulnerability in 2023, followed by Remote Code Execution. This isn't surprising as it parallels directly with known threat tactics.

Two primary threat actor tactics are:

1. Getting their code to execute (https://attack.mitre.org/tactics/TA0002/)
2. Gaining access to the privileges needed to follow through on their objectives (https://attack.mitre.org/tactics/TA0004/)

The good news this year is that, while Elevation of Privilege vulnerabilities remain the #1 vulnerability category, they have decreased from 715 to 490—a substantive 31% drop. When we dive into the data, we can clearly see those reductions are primarily coming from reductions in Azure and Windows Server vulnerabilities, as shown in the figure below.

This is welcome news, given that these systems are often public-facing and much more likely to contain large amounts of sensitive data and privileged service accounts than, for example, a Windows Desktop system.



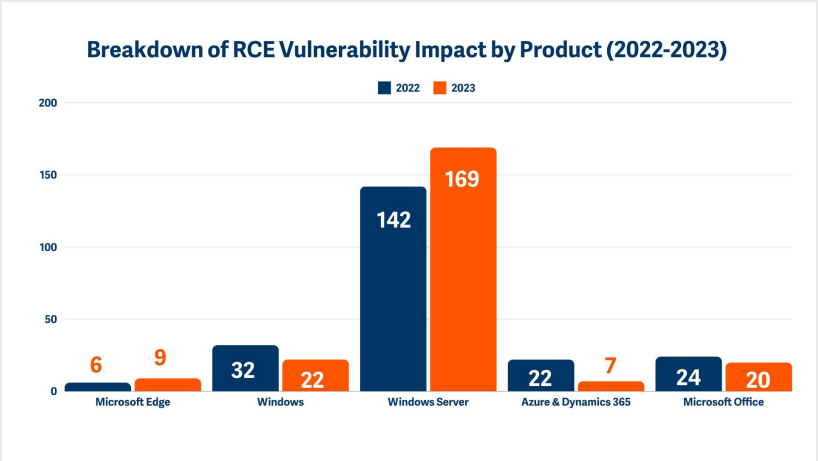
Azure and Windows Server both show a significant reduction in EoP vulnerabilities. Azure dropped from 72 EoP vulnerabilities in 2022 down to 10 in 2023 (a massive 86% decrease), and Windows Server dropped from 191 to 141 (a 26% decrease).

In general, the reduction of Elevation of Privilege vulnerabilities is a very positive trend that directly reduces a threat actor's options when deploying a threat that requires elevated privileges to run.

However, you can't just rely on a lack of Elevation of Privilege vulnerabilities to protect access to privileges. It is still essential to maintain a robust Privilege Access Management strategy to remove and secure privileges within an environment to prevent them from falling into the hands of an attacker.

Remote Code Execution a close second to Elevation of Privilege in 2023

Coming in a close second place is the Remote Code Execution (RCE) vulnerability category, which rose from 314 to 356 in 2023 (13% increase). While in many product areas, such as Azure, Office, and Windows (now mainly consisting of Windows 10 and 11 data), we have seen RCE decrease, this was offset this year by an increase on the Windows Server side.



Windows Server RCE vulnerabilities jumped from 142 to 169 in 2023, a 19% increase.

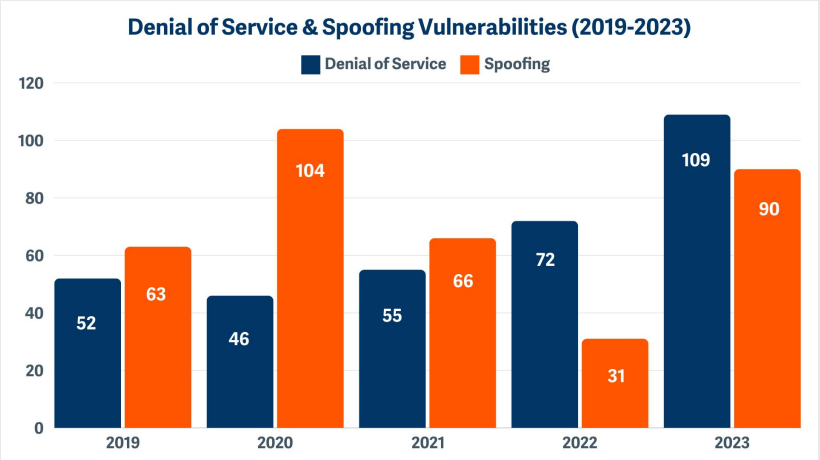
The increase in Windows Server RCE vulnerabilities is not caused by one particular component, but is broadly spread across different services and features. In fact, many of these detections resulted from Microsoft's increased collaboration with their security research community. Notably, it appears this collaboration is paying off because many of these vulnerabilities were disclosed directly to Microsoft and patched before they were publicly disclosed or observed being exploited in the wild.

Risk, reverse engineering, and researchers - the race continues.

Timely patches allow organizations to keep ahead of the majority of threat actors—provided organizations deploy the patches in a timely manner. Once a vulnerability is disclosed and patches are released, the race is on to successfully patch before a threat actor reverse engineers the patch or the vulnerability gets publicly disclosed, allowing for the creation of exploits in the wild.

Both researchers and threat actors have had success in reverse engineering patches to find exploitable workarounds or other vulnerabilities in recently patched areas of code. As the saying goes, there is no smoke without fire, and as we highlighted in last year's report, vulnerabilities can start to snowball when attention is drawn to an area that might contain multiple exploitable areas of code.

Denial of Service and Spoofing vulnerabilities jump significantly in 2023



Denial of Service vulnerabilities hit a record high in 2023, climbing 51%, from 72 in 2022 to 109 in 2023, with Spoofing demonstrating a dramatic 190% increase, from 31 in 2022 to 90 in 2023.

When thinking about information security, we often focus on ensuring the confidentiality and integrity of data, but disrupting the availability of data can also have a devastating impact. Denial of Service (DoS) exploits can be used to disrupt the availability of data and cause challenges to business operations in a similar way as ransomware.

What can we learn from this year's vulnerabilities categories?

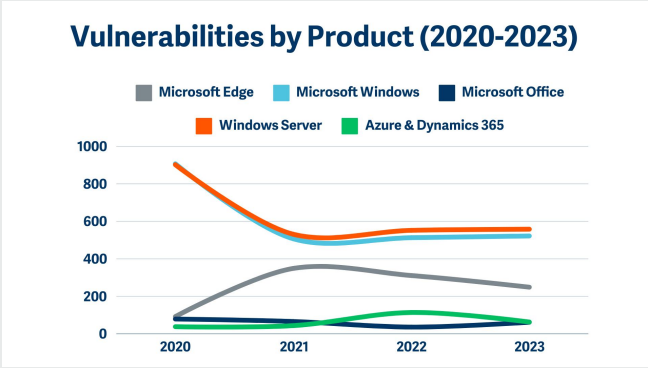
As overall vulnerabilities stabilize, threat actors shift focus to identities.

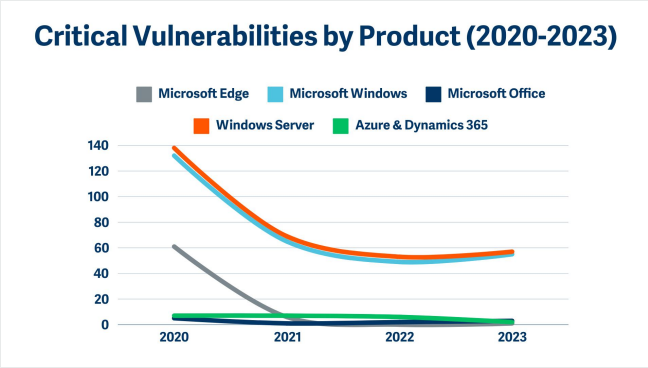
When it comes to getting code to run, threat actors have choices beyond exploiting vulnerabilities. They can use social engineering or stolen credentials to introduce their code into an environment without the need for a software vulnerability. Similarly, when it comes to elevating privileges, it might be easier to hijack an already-privileged account than exploit a software vulnerability or a misconfiguration in the environment to access the privileges required.

As the overall number of Microsoft vulnerabilities stabilizes and the number of critical vulnerabilities decreases, we see that attackers, much like water, will flow to the path of least resistance and focus much more of their attention on identities.

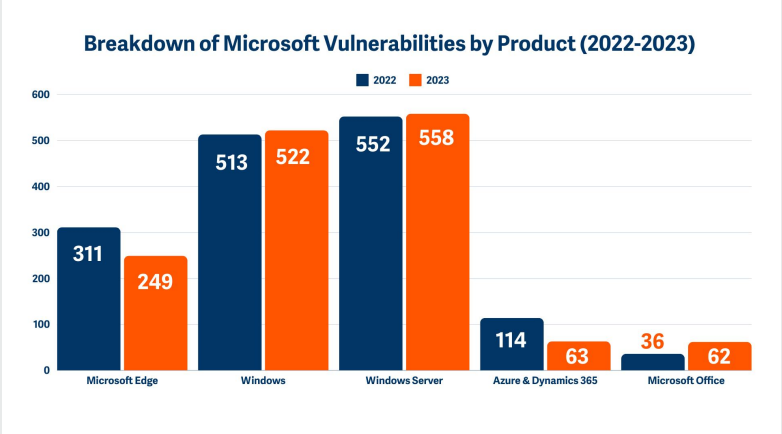
However, this doesn't mean we can become complacent about software vulnerabilities. Not only are there plenty of vulnerabilities to go around, but there are also a number of unpatched systems still vulnerable to exploits that had patches made available months or years ago. These known vulnerabilities make it all too easy for threat actors to launch a successful attack.

Vulnerabilities by Product

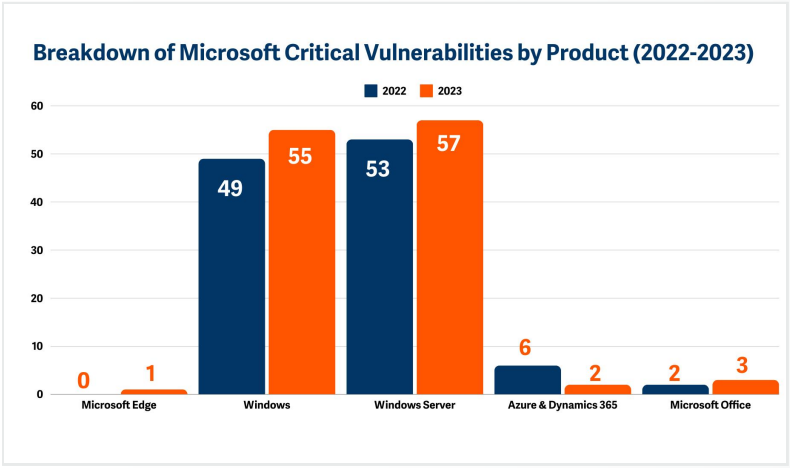




Overall, vulnerability numbers have stabilized. Total vulnerabilities continue a four-year plateau, and critical vulnerabilities continue to decline, although the descent has slowed.



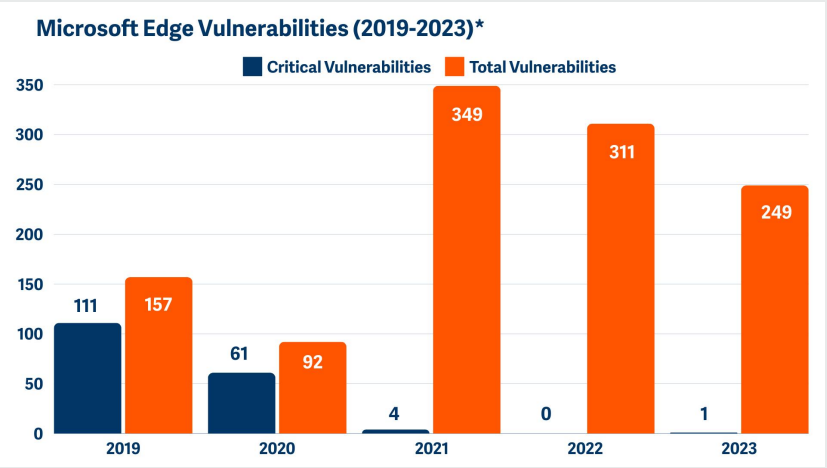
Windows Server vulnerabilities increased slightly in 2023. Total vulnerabilities increased slightly from 552 to 558 (1%). Critical vulnerabilities saw a similarly slight increase, from 53 to 57.



The Windows vulnerability category showed a similar pattern, with total vulnerabilities increasing from 513 to 522 (2%), and critical vulnerabilities increasing from 49 to 55.

Office and Edge continue to lead the way, and Azure course-corrects after a record-breaking vulnerability spike in 2022.

Microsoft Edge continues downward vulnerability trend.



Chromium code base continues to offer significant security improvements, marked by a three-year plummet of vulnerabilities and exploits.

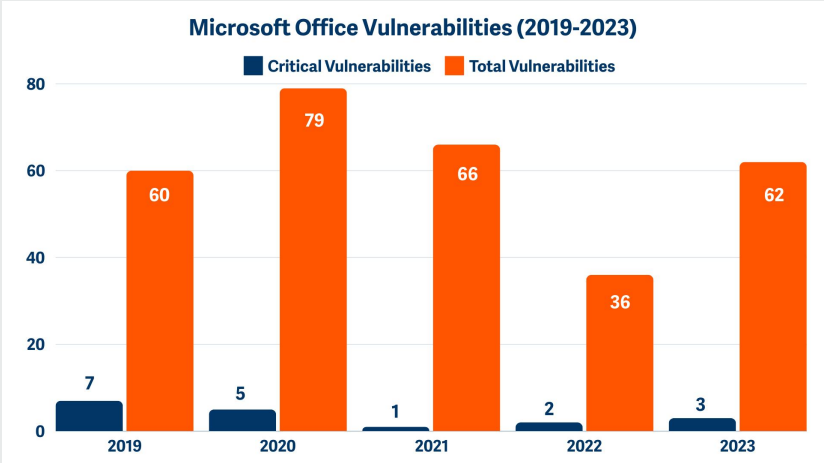
*2019-2021 includes Internet Explorer, which was discontinued last year. 2022/23 figures are Edge only

Web browsers and document viewers have historically been a major pain point when it comes to vulnerabilities and cyberattacks. Fortunately, Microsoft has made significant strides in maturing the security of these areas.

On the browser side, moving Edge away from a custom Microsoft codebase and over to a Chromium code base has yielded significant security improvements. Removing support for Internet Explorer has also helped, making drive-by download exploits and vulnerable Flash plugins a thing of the past.

Critical vulnerabilities in Microsoft Edge have plummeted from 162 in 2017 to only 1 in 2023 (and 0 in 2022). This is largely due to the adoption of the security maturity offered by Chromium, which is used as the base for multiple web browsers.

Microsoft Office vulnerabilities jump back up to 2019-2021 levels in 2023



Office vulnerabilities increase over 2022, but continue an overall downward-leaning trend, forcing attackers toward more innovative attack methods.

On the Office side of the house, we have seen a similar (although not quite so dramatic) downward trend for both total and critical vulnerabilities, despite an increase in 2023. Again, this is partly due to some of the older versions of Office coming to End-of-Life (EoL) and no longer being supported.

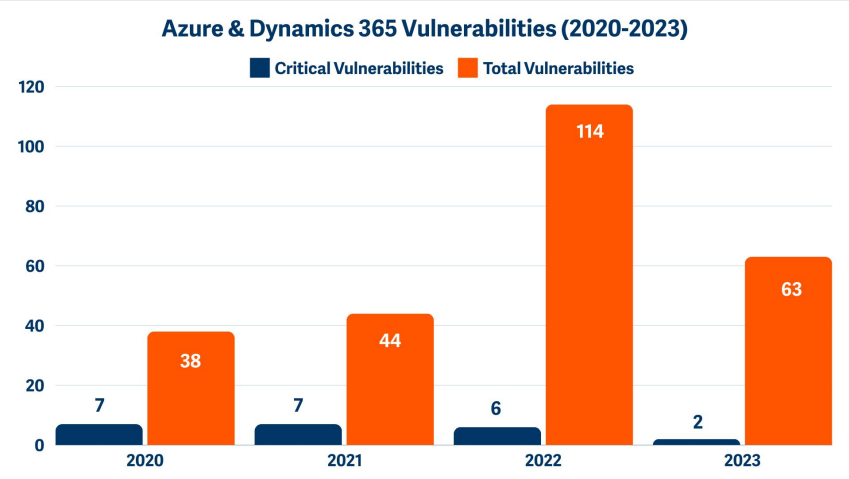
Efforts to prevent common phishing and malware payloads via Office applications continue to force attackers to innovate. Controls introduced to disable macros from auto-running in downloaded documents have stymied some common paths to Remote Code Execution, forcing threat actors to look for more creative ways to run code using malicious documents and files.

One of the more interesting new areas for vulnerabilities within Office applications comes from Microsoft adding support for SketchUp Software's proprietary SKP files in June 2022. This was designed to make it easier to import 3D models into Word, Excel, PowerPoint, and Outlook. Unfortunately, adding 3D file support to documents also introduced a new dimension to the vulnerability landscape, with the team at ThreatLabz discovering 117 unique vulnerabilities that got rolled up into CVE-2023-33146, CVE-2023-28285, and CVE-2023-29344.

Microsoft went on to create a patch to address these vulnerabilities, which the team at ThreatLabz was able to bypass. This resulted in Microsoft temporarily disabling support in Microsoft 365 for SketchUp files in June 2023.

While Microsoft has supported 3D file formats for a while now, this incident reinforces how any addition of new features can introduce security vulnerabilities. In this case, the additional code added to the MSOSPECTRE.DLL library, which is responsible for parsing 3D file formats, exposed vulnerabilities that Microsoft hadn't anticipated.

Azure & Dynamics 365 vulnerabilities nearly halved in 2023.



After spiking in 2022, Azure & Dynamics 365 vulnerabilities saw an impressive 45% decrease from 114 to 63 in 2023.

After Microsoft Azure and Dynamics 365 vulnerabilities skyrocketed in 2022, they almost halved in 2023—down from 114 to 63. Considering the vast number of products and services this product area covers, the numbers are impressively low.

In last year's report, we highlighted a cloud migration tool that caused a substantial proportion of the vulnerabilities largely associated with SQLi type vulnerabilities (who would have thought we would still be talking about SQLi today!).

In 2023, this upward trend has course-corrected back to the level we would expect to see. This product area is predominantly newer code being developed entirely using the Microsoft Secure Development Lifecycle, and we can clearly see the benefits as compared to legacy products, which generally have higher rates of vulnerabilities.

> "Proactive security hardening often breaks your attacker's exploit chain, keeping a single phished account from giving your attacker domain admin."
>
> **Jay Beale, CEO, CTO, InGuardians, Inc.**

Vulnerabilities Spotlight

Understanding the methods threat actors are using to exploit vulnerabilities and infiltrate organizations can help you make more informed decisions to protect your organization.

Print Spooler Snowball Slows

The goldrush of vulnerabilities—and prime targets for Elevation of Privilege attacks—may be nearing its end, but that doesn't mean threat actors can't still cash in.

2018
"The Printer Bug" is identified. This bug allows an unprivileged user in the network to remotely trigger the Domain Controller's Print Spooler service to authenticate to an arbitrary system. This bug allows the attacker to impersonate the Domain Controller.

2019
"The Printer Bug" becomes CVE-2019-0683 and casts attention to the Print Spooler service.

2020
Seven (7) Windows Print Spooler Elevation of Privilege vulnerabilities are disclosed. Initially, these vulnerabilities are all local attack vectors, requiring the attacker to first have direct access to the system running the Print Spooler. However, the outcome of each is that an attacker could run arbitrary code with elevated system privileges.

CVE-2020-1030
CVE-2020-1048
CVE-2020-1070
CVE-2020-1337
CVE-2020-17001
CVE-2020-17014

CVE-2020-17042
Appears in late 2020. Unlike previous exploits that were locally exploitable, this one is remotely exploitable, meaning the attacker need only be on the network. This RCE attribute makes this particular vulnerability much more severe. However, this vulnerability had not been publicly disclosed and was not known to be used as an exploit in the wild before it was patched.

The Vulnerability Snowball Effect

This phenomenon occurs when one vulnerability is found and patched, but the process draws the fresh scrutiny of new researchers who find new vulnerabilities, new attack vectors, and new ways around previous patches—causing the vulnerability count to snowball.

The Print Spooler service, which contains code that is over 20 years old, is a poignant example of the vulnerability snowball effect in action.

2021

16 Windows Print Spooler Elevation of Privilege vulnerabilities are disclosed. The Print Spooler is now catching the eye of many researchers as an interesting way to perform Elevation of Privilege attacks.

The number of disclosed Windows Print Spooler EoP vulnerabilities rapidly unspools as Microsoft plays Whack-A-Mole with researchers who have found ways around patches and continue to exploit vulnerabilities.

CVE-2021-34527 is the most noteworthy of the 2021 class of Windows Print Spooler EoP vulnerabilities.

This vulnerability is very straightforward to exploit.

A network needed little more than a valid user account and the Print Spooler to allow remote connections (which are enabled by default). The ease of exploit, combined with the fact it had been publicly disclosed and was actively being used in the wild, earned it the name "Print Nightmare."

The other 15 such vulnerabilities in the 2021 class include: CVE-2021-41333, CVE-2021-41332, CVE-2021-40447, CVE-2021-38671, CVE-2021-38667, CVE-2021-36970, CVE-2021-36958, CVE-2021-36947, CVE-2021-36936, CVE-2021-34483, CVE-2021-34481, CVE-2021-26878, CVE-2021-1695, CVE-2021-1675, and CVE-2021-1640.

2022

35 Windows Print Spooler Elevation of Privilege vulnerabilities are disclosed, more than doubling what was recorded the previous year.

CVE-2022-44681, CVE-2022-44678, CVE-2022-41073, CVE-2022-38028, CVE-2022-38005, CVE-2022-35793, CVE-2022-30226, CVE-2022-30206, CVE-2022-30138, CVE-2022-29140, CVE-2022-29132, CVE-2022-29114, CVE-2022-29104, CVE-2022-26803, CVE-2022-26802, CVE-2022-26801, CVE-2022-26798, CVE-2022-26797, CVE-2022-26796, CVE-2022-26795, CVE-2022-26794, CVE-2022-26793, CVE-2022-26792, CVE-2022-26791, CVE-2022-26790, CVE-2022-26789, CVE-2022-26787, CVE-2022-26786, CVE-2022-23284, CVE-2022-22718, CVE-2022-22717, CVE-2022-22041, CVE-2022-22022, CVE-2022-21999, and CVE-2022-21997

2023

5 Windows Print Spooler Elevation of Privilege vulnerabilities are disclosed, a significant reduction over previous years.

CVE-2023-35325, CVE-2023-35302, CVE-2023-21765, CVE-2023-21760, CVE-2023-21678

In last year's report, we talked about the snowball effect around Windows Print Spooler vulnerabilities, where the over 20-year-old code that had been passed down through versions of Windows had started to show its age and become a target for exploits. Print Spooler vulnerabilities had roughly doubled in number every year since the 2019 discovery of "The Printer Bug" CVE-2019-0683, peaking in 2022 with 35 vulnerabilities.

This goldrush seems to have now settled down to a mere five vulnerabilities in 2023: CVE-2023-35325, CVE-2023-35302, CVE-2023-21765, CVE-2023-21760, CVE-2023-21678

As encouraging as it is to see the volume reduce, these are not insignificant vulnerabilities, and the majority are associated with Elevation of Privilege. Given that the print spooler service runs as SYSTEM (the highest level of privilege within the Windows OS), it is a prime target for Elevation of Privilege exploits.

Unlike previous years, it appears Microsoft managed to issue patches before any of these vulnerabilities were publicly disclosed or exploited in the wild. This provides some reassurance that lessons in this area have been learned, but still demonstrates that now is not the time to get complacent.

Time to say "goodbye"

End-of-Life (EOL) software is no longer supported or patched, making it an elevated risk to organizations and a prime target for threat actors.

Many Microsoft products met an End-of-Life (EOL) fate in 2023. This means that they will no longer receive security patches to address vulnerabilities or other issues.

Notable this year is the EOL of Server 2012 and Server 2012R2. As a parting gift, both server operating systems received a retirement package of 65 patches, with 11 of those being critical. To incentivize cloud migrations to Azure for those still using these operating systems, Microsoft is offering three years of Extended Security Updates (ESUs) beyond the end of the support date (Oct 2023) on Azure.

At the other end of Microsoft's Extended Security Updates (ESU) program is Windows 7. The OS you probably already thought was long gone is now no longer covered by Microsoft's ESU program. Since this means no more access to critical security patches, it's definitely time to accelerate plans to move any legacy Windows 7 systems forward.

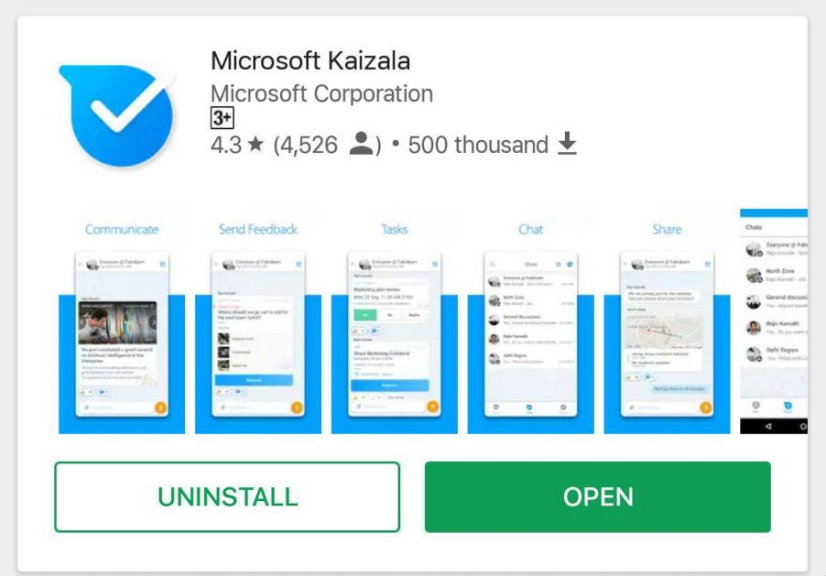


Fig. 4: Microsoft Kaizala is one of many Microsoft products to meet an End-of-Life (EOL) fate in 2023.

There were also a few products that, much like the Microsoft Zune mp3 player, failed to really take off, and have been retired without much attention. So, in 2023, we said farewell to Microsoft Kaizala. Your 2G network-optimized secure messaging is now part of Teams and has been forced to retire.

Outlook is out of luck with CVE-2023-23397

A dangerous combination of ease of exploitability and high impact caused this vulnerability to grab the attention of IT administrators—and threat actors—in 2023.

While we are continuing to celebrate an all-time low of critical vulnerabilities across Microsoft products, there are still some eyebrow-raising critical vulnerabilities that struck fear into the hearts of IT professionals in 2023.

Unlike many past vulnerabilities, CVE-2023-23397 in Microsoft Outlook requires no user interaction to trigger the exploit. Worse still, the vulnerability impacted all versions of Microsoft Outlook for Windows and allowed an attacker to gain sensitive Windows New Technology LAN Manager (NTLM) credential hashes. This dangerous combination of ease of exploitability and high impact resulted in a base CVSS score of 9.8, which is more than enough to get the attention of IT administrators and threat actors alike.

The vulnerability is triggered when an attacker sends a specially crafted calendar invite or appointment to a target victim's email address. This invite contains additional properties that cause Outlook to make an SMB connection and trigger NTLM authentication to a server on the internet that is under the attacker's control. From there, the attacker can capture the NTLM hashes and use them to authenticate themselves as the victim, leading to potential escalation of privileges and further compromise of the environment.

The real danger is that the underlying vulnerability is triggered without the user having to open the invite at all. In fact, the trigger is the reminder notification sound.

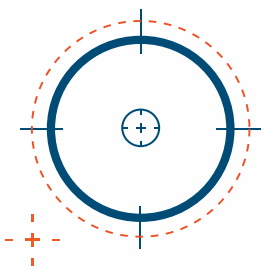
While this is usually a predictable "ping" sound to remind you a meeting is about to happen, there is a "PidLidReminderFileParameter" property which can be used to specify a custom audio file to play. This property can be abused. If an attacker sets it to be a remote resource under the attacker's control, it will cause Outlook to connect and authenticate, ultimately revealing the hashes for the victim's credentials.

As we highlighted in last year's report, impactful vulnerabilities such as this often draw the attention of threat actors and the research community alike, resulting in a game of Whack-A-Mole as Microsoft tries to release patches faster than workarounds are discovered. Researcher Dominic Chell quickly uncovered that the patch released for CVE-2023-23397 only fixed the issue for remote access, and if an attacker was within the network, they would still be able to exploit this vulnerability.

While mitigations, such as blocking outgoing SMB connections or adding users to the Protected User Group to prevent the use of NTLM authentication, are available, this is a critical vulnerability to patch given the ease with which it can be exploited.

Because the vulnerability allows an attacker to capture and potentially replay NTLM hashes to authenticate as the target victim, **it is important to always honor the principle of least privilege. The fewer privileges the victim has, the lower the risk of account and identity compromise.**

In the worst case, you would have a domain administrator checking emails from a highly privileged account, giving an attacker an easy path to take over the entire domain. In an ideal scenario, you would have removed local admin privileges and properly secured highly privileged accounts, such as domain administrators, to ensure that, no matter what vulnerability was exploited, the impacts would be mitigated.



It is important to always honor the principle of least privilege. The fewer privileges the victim has, the lower the risk of account and identity compromise.

Russian RomCom misses the mark with CVE-2023-36884

These elaborate phishing campaigns targeted defense and government entities with malicious attachments that leveraged a zero-day Remote Code Execution exploit to evade Mark of the Web protections. This is a clear example of how attackers have been innovative in bypassing protections as Microsoft continues to improve default Office security.

A phishing campaign in the summer of 2023, attributed to Russian cybercriminal group RomCom (also referred to as Storm-0978), targeted defense and government entities in Europe and North America with lures relating to the Ukrainian World Congress.

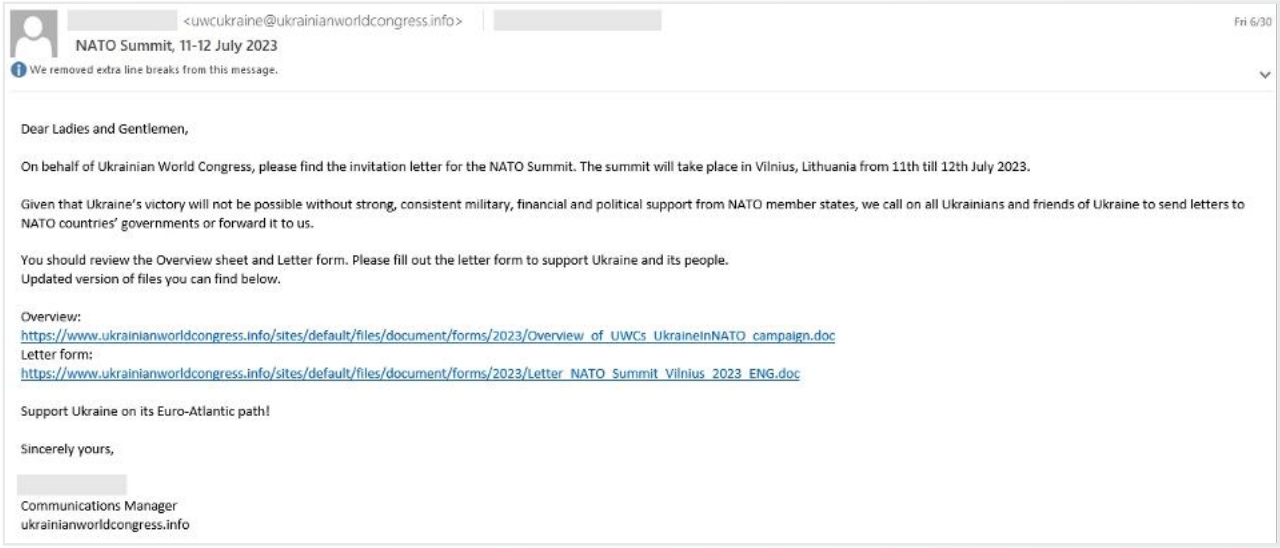


Figure 5: A screenshot of the 2023 phishing campaign launched by Russian cybercriminal group RomCom

The objective of the phishing lures was to manipulate their targets into downloading and opening the malicious documents linked from the email.

It is worth noting that the attackers often separate the malicious payload from the phishing email using links within the email or within an attached document. This makes the malware harder to detect because the malicious code is hidden within the email. When the email is analyzed and security solutions attempt to scan these links, they can be blocked or redirected by the server hosting the payloads.

RomCom specializes in this type of phishing attack. The group previously compromised a Ukrainian Ministry of Defence email account in late 2022. Their purpose during this attack was to send phishing emails with PDF attachments containing links to compromised websites that host information-stealing malware.

While the use of malicious Office documents is nothing new, this campaign was noteworthy for exploiting a vulnerability that later became known as CVE-2023-36884.

To protect users against malicious documents, Microsoft attaches a Zone Identifier tag, known as the "Mark of the Web," to files downloaded by browsers and email clients. This tag contains a Zone ID that indicates whether the file was downloaded from the internet or local network, as well as the URLs it originated from.

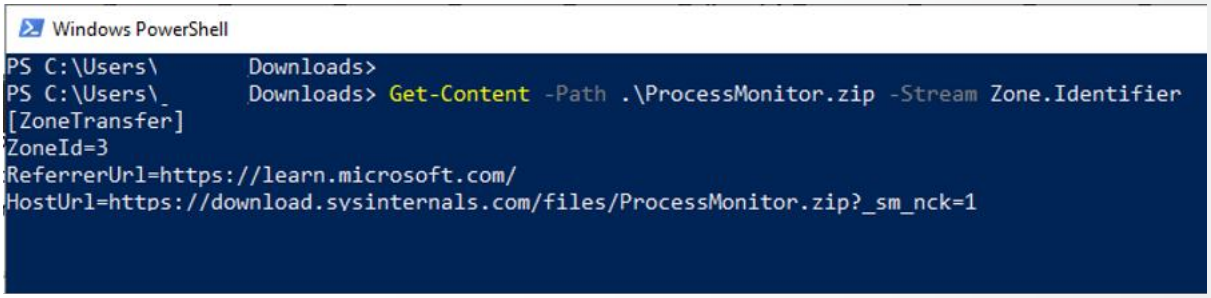


Figure 6: Using PowerShell to view the Mark of the Web on a downloaded file.

This Mark of the Web (MotW) is then used by Microsoft Office, Microsoft SmartScreen, and other security tools to apply restrictions, such as preventing potentially malicious macros in a Word document from automatically executing.

In this case, RomCom had discovered a zero-day Remote Code Execution exploit to evade the Mark of the Web protections. They exploited a Windows Search feature to download remote files onto the local filesystem where, for a brief time, they were not tagged with the MotW. This effectively bypassed the MotW protections, allowing the attacker to execute actions that would normally be prevented for content downloaded from the internet. The threat actors were then able to initiate a chain of events that ended in arbitrary code execution.

Interestingly, the structure of the malicious documents used by RomCom contains elements of the Follina exploit (highlighted in last year's report), with analysis linking it to CVE-2022-30190, a vulnerability that was also used to bypass Office document security controls. As Microsoft has improved the default security of Office, attackers have continued to innovate in bypassing the protections.

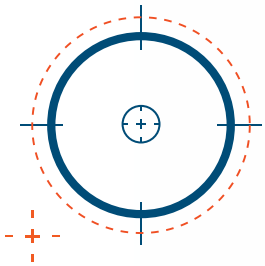
This exploit was not alone. In 2023, researchers from Palo Alto Networks also discovered CVE-2023-36584, which used a different exploit vector to also bypass MotW protections.

This steady stream of Remote Code Execution vulnerabilities in Office highlights that, even with these recent Microsoft security enhancements, attackers are still finding ways to execute code.

Many organizations struggling with historic Office vulnerabilities, and security features that aren't enabled by default, might feel like the battle is lost. However, as with all Remote Code Execution vulnerabilities, the principle of least privilege is a key defensive measure.

Ultimately, no matter what the exploit is, the malware payload will run in the context of the user who opened the document. If that user has administrator privileges, then so will the threat actor.

But if you remove the privileges and layer in application control, then you can proactively mitigate the threat—even when a zero-day exploit is used.



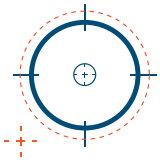
The principle of least privilege is a key defensive measure. No matter what the exploit is, if you remove privileges and layer in application control, you can proactively mitigate the threat—even when a zero-day exploit is used.

Are organizations having an identity crisis?

Increasingly, attackers are re-focusing their efforts on exploiting identities, rather than Microsoft software vulnerabilities. Midnight Blizzard represents a prime example of what can happen when threat actors get innovative with identity-based infiltration tactics.

Some time ago, Morey J. Haber, Chief Security Advisor at BeyondTrust, posed the question, "Are we having an identity crisis?" At first, the play on words caught us off guard, but we quickly realized that his question was a pun based on the growing challenges organizations face around managing identities and identity security.

As a Chief Security Advisor and former CSO and CTO, Morey has been tracking the rising tide of identity threats, while also helping others understand the complex challenges and threat landscape. His new book, ***Identity Attack Vectors: Strategically Designing and Implementing Identity Security***, provides a thorough assessment of the challenges of implementing real identity security within an organization.



"[Y]our identity crisis is not a personal one, but rather describes a problem with how you manage identities and identity security within your organization."

Morey J. Haber,
Chief Security Advisor,
BeyondTrust

Given that this report is designed to help organizations better understand the threat landscape around the Microsoft ecosystem and beyond, it is important to address this identity crisis—and the fact that attackers are shifting more emphasis onto identity-based attack vectors.

How to Identify an Identity Crisis in Your Microsoft Ecosystem:

Key Questions Based on Identity Attack Vectors

What does an identity crisis in your Microsoft ecosystem look like?

It looks like a user logging in, and that is what makes it so difficult.
You can have fully patched systems and great security tooling, but if an attacker is able to steal credentials, hijack a session token, or socially engineer the help desk, they may be be able to walk straight into your environment. In a world where it is easier to log in than hack in, identity becomes the new perimeter.

It looks like vulnerabilities, process issues, and risks associated with the identity-account relationship.
The risks themselves can be diagnosed by identifying flaws in the joiner, mover, and leaver process and the permissions, rights, privileges, roles, entitlements, authentication (like multi-factor authentication (MFA) and Single Sign On (SSO)), and authorization for identities and accounts at rest and operating during runtime.

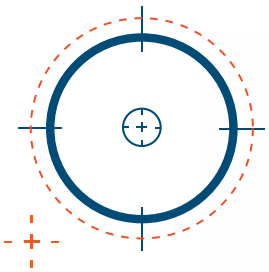
What turns a security challenge into an identity crisis?

The detections and recommendations needed to classify the risks are generally buried deep in the data. Without a clinical approach to the problem, the symptoms often go unnoticed, unless a security professional is specifically threat-hunting for them.

Many security teams' mindsets have become focused on chasing down and detecting threats when, in reality, there is a need to become more proactive. When it comes to the identity crisis, vulnerabilities might not be flaws in the underlying code.

The vulnerability could be a misconfiguration in Active Directory that allows any user to elevate their privilege. It could also be a combination of obscure Entra ID roles that allows an attacker to add credentials to a privileged OAuth app that can access corporate mailboxes.

> "Prevention is key, but you can never avoid everything. You need detection, too."
>
> **Jay Beale, CEO, CTO, InGuardians, Inc.**



Attackers think in complex graphs to navigate pathways through Microsoft systems.

> **There's a fairly famous saying in security:**
> "Defenders think in lists. Attackers think in graphs. As long as this is true, attackers win."
>
> John Lambert,
> Corporate Vice President, Security Fellow,
> Microsoft Security Research.

The idea is that a defender thinks in siloed lists:

- Defender A thinks about Active Directory,
- Defender B thinks about Windows Desktop AV,
- Defender C thinks about Windows Servers, etc.

The attacker, on the other hand, thinks about a graph, or series of connections between accounts and systems that they can use to achieve their objective. They exploit the lack of visibility between these disparate systems (the defender's lists) to move laterally and inflict damage. That could mean starting on Windows Desktop with a local admin privileged user, then using that access to capture a privileged domain account and pivot onto a server.

> **We need to be able to think in graphs**, just like attackers do. If we can gain more holistic visibility of all the accounts, privileges, and access in our environment, then we can start to break out of our silos and lists to see what attackers see and what they can exploit in our environments.
>
> We can understand and remediate paths to privilege, vulnerabilities, and misconfigurations. While this is easier said than done, it is vital to be able to tip the balance in favor of the defenders and stay ahead of threats.

As an industry, we need to start thinking more holistically about privileges, identity hygiene, and identity threat detection.

The core messages that have resonated through this report for the past 11 years—enforcing least privilege, hardening configurations, and the importance of patching—represent some of the core strategies needed to defend against cyber threats. These core messages are equally applicable to the identity crisis. It doesn't matter if an account is compromised via a session hijack on the cloud or an exploited vulnerability on an endpoint—the fewer privileges and access the compromised user has, the more the risk is reduced.

Let's take a look at how Microsoft was impacted by their own identity crisis in 2023.

Microsoft gets tested by Midnight Blizzard

Attackers orchestrated a masterful attack, leveraging identity-based infiltration tactics and often-unnoticed privileges and access to navigate a path through Microsoft's systems.
The Midnight Blizzard attack exemplified how it's easier for attackers to log in with a stolen account than to hack in by exploiting a vulnerability.

A prime example of a modern identity-based attack occurred when Microsoft was targeted by the threat actors known as Midnight Blizzard (also Cozy Bear and APT29). This attack doesn't appear to have involved any of the software vulnerabilities that we traditionally cover in this report. Instead, it was a masterclass in **attackers thinking in graphs**, and using often-unnoticed privileges and access between accounts and systems to navigate a path through Microsoft's systems.

The attack started in 2023, when an account in a non-production test environment was subject to a password spray attack. Unfortunately, the targeted Entra ID account did not have multi-factor authentication (MFA) enabled. This meant, once the attackers had successfully guessed the password, they had access to the account.

It appears that the compromised account, while not directly overprivileged, had the ability to create new secrets for OAuth applications within the test environment. At this point, the attacker should have been limited to the test environment, but this was not the case. Microsoft stated that, within the test environment, there was a "legacy test OAuth application that had elevated access to the Microsoft corporate environment." This meant the attackers had the ability to add secrets, authenticate as the privileged test application with elevated access to the corporate environment, and then execute commands.

With this expansive level of access, the attackers could create a new malicious OAuth application and grant it the "full_access_as_app" Microsoft 365 Exchange Online permission for the corporate environment. This permission allowed the attacker to access the mailboxes of senior executives using credentials assigned to their malicious OAuth application.

This attack is a fitting example of how the threat landscape is evolving toward a tipping point: **it is becoming easier for attackers to log in with a stolen account than hack in by exploiting a vulnerability.**

As we have shown in the 11 years this report has been running, the landscape is constantly evolving.

With Microsoft's investments in securing their software and reducing the number of critical vulnerabilities, combined with the push to the cloud making data and systems accessible from any network, **we can only assume that the volume and sophistication of identity security threats is going to substantially increase in the next decade.**

> "Midnight Blizzard was another case of the popular adage, 'Attackers don't break in - they log in'."
>
> **Jay Beale, CEO, CTO, InGuardians, Inc.**

What Do the Experts Say?

Paula Januszkiewicz

CEO
CQURE

We're all witnessing a shift in the importance of cybersecurity in everyday life. For a long time, it has been a niche concern reserved for tech enthusiasts. Today, it's become a vital aspect of daily reality for individuals and businesses alike. As the world becomes increasingly digital, the stakes in protecting our data and privacy are higher than ever. The insights from BeyondTrust's Microsoft Vulnerabilities Report 2024 serve as a reminder of the ever-present challenges we face.

Paula's commentary continued on next page >

2023 was the year of AI, generative AI, and automation, which will keep revolutionizing the way we approach cybersecurity in the years to come. These technologies offer incredible potential in detecting and mitigating threats, providing support in our defense strategies, and making the work of SecOps teams more manageable. However, they also introduce new challenges, such as deepfakes and sophisticated disinformation campaigns. AI has quickly become a double-edged sword—a powerful tool serving both sides.

The 2024 Microsoft Vulnerabilities Report brings to light a nuanced picture of the current state of vulnerabilities. On a positive note, critical vulnerabilities have seen a slight decrease, continuing a hopeful trend. Also, the number of Elevation of Privilege vulnerabilities (top vulnerability category) has dropped substantively, most likely thanks to the work in Azure and Windows Server vulnerabilities. Yet the overall number of vulnerabilities within Microsoft's ecosystem remains steady, a concerning signal that, despite all the efforts and investments, the threat landscape is far from diminishing. The marked increase in spoofing vulnerabilities particularly stands out, underscoring the constant need for vigilance.

Refining our approach to cybersecurity is a crucial task. This includes stricter control over privileges, hardening security protocols, and tailoring our defenses to our environments' characteristics. The key is to stay informed about emerging threats, deploy effective detection and response mechanisms, regularly perform audits and penetration tests, and continually review and test our incident response plans. These principles resonate deeply with our own experiences, reinforcing their critical role in maintaining a strong cybersecurity framework.

We should not forget, however, that at the heart of cybersecurity remains the human element. The most advanced technological defenses can be compromised by simple human error. This report notes a shift happening now: stealing identities is becoming easier than exploiting a vulnerability. As a consequence, identity-based attacks will likely become even more common in the near future.

Hence, fostering a culture of awareness and education among all users is crucial. Unlike hacking, which is often a solitary job, cybersecurity is inherently a collaborative effort. This perspective, echoed in the report, highlights the importance of a people-centric approach to cybersecurity.

Reflecting on the insights gathered in BeyondTrust's report, it's clear that the journey ahead in 2024 will require us to adapt and rethink our cybersecurity strategies. As adversaries become more sophisticated, integrating cybersecurity more deeply into our daily routines and business operations will be vital. The key to navigating the future will be a balanced approach that combines technological innovation with a strong commitment to education and cooperation.

My advice? Stay vigilant, embrace the change, constantly learn from the community, and don't forget to give back. This way, we can ensure a safer future for all.

David Morimanno

Director of Identity & Access Management Technologies, Integral Partners, a Xalient Company

The findings of this year's Microsoft Vulnerabilities Report confirm what we've seen in the contemporary cybersecurity landscape. As cybercriminals increase their focus on identity-centric vulnerabilities, a robust Identity and Access Management program plays a critical role in mitigating evolving threats. This is particularly true for threats centered on identity vulnerabilities within the Microsoft ecosystem, facilitated by the expansion of cloud platforms like Azure and Microsoft 365. Complex, interconnected systems introduce unforeseen vulnerabilities, necessitating a proactive approach to identity-centric security measures.

Implementing zero trust principles has become a key focus for many of the organizations we work with, as has building an identity fabric. An identity fabric is a paradigm for a comprehensive set of identity services, delivering the capabilities required for providing seamless and controlled access for everyone to every service. Integrating Privileged Access Management into the broader identity fabric is imperative for fortifying security measures and averting potential cyberattacks.

Why has the number of vulnerabilities reported stayed flat?

In this report, the number of Microsoft vulnerabilities has stayed relatively flat. Why is that? Microsoft's efforts to promptly patch known vulnerabilities may be offsetting the discovery of new ones by reducing the window of opportunity for attackers to exploit vulnerabilities. Also, as the MS codebase matures, new vulnerabilities might be getting introduced at a slower rate. Another possibility is that Microsoft products often rely on third-party libraries and components, which could introduce vulnerabilities that aren't directly attributable to Microsoft's code.

The importance of PAM and its contribution to the identity fabric

The CVE-2023-23397 incident underscores the dangers of password reliance and inadequate access controls. The zero-click exploit didn't require user interaction, allowing a vulnerable system to be compromised via an unopened email! Such attacks emphasize the need for multi-factor authentication (MFA), segmentation, least privilege, and timely patching to mitigate similar risks. PAM obviously plays a crucial role in mitigation as part of a holistic identity-centric program that strengthens your broader Identity Fabric, encompassing IGA, Access Management, Directory Services, and Cloud Infrastructure Entitlements Management (CIEM).

David's commentary continued on next page >

One of the many tools we utilize in our advisory practice to help organizations effectively address identity-related risks is a comprehensive identity risk assessment checklist, encompassing facets such as governance, lifecycle management, privileged access, and machine identities.

We also emphasize the need to leverage artificial intelligence (AI) where possible. The future of identity-centric security will no doubt leverage advanced technologies like artificial intelligence and behavioral analytics to detect and respond to threats in real-time, ensuring that organizations remain resilient in the face of ever-evolving cyber risks.

Greg van der Gaast

Managing Director
Sequoia Consulting
sequoia-consulting.co.uk
greg@sequoia-consulting.co.uk

Greg van der Gaast is Managing Director at Sequoia Consulting, a specialist security advisory that focuses on addressing business and process issues so that you have fewer security ones.

"The value in vulnerabilities"

I thought I might contribute with practical advice on how to leverage your vulnerabilities more strategically and look at things more important than a CVSS rating.

If we want to make progress in improving our organisation's security posture, rather than firefighting, we need to worry less about what vulnerabilities we have and more about why we have them.

For example, having the hypothetical 9.8 CVSS score CVE that came out yesterday doesn't really concern me. My patching process should handle that operationally within 24-48 hours.

If this isn't the case for you, I'd suggest you spend more time maturing your patching programme. If there are reasons why we can't patch, we should ask ourselves why those reasons exist, whether they strictly need to, and what we can do to change that.

The latest, greatest, big, scary CVEs don't worry me. What worries me is the two-year-old "low risk" vulnerability. Its presence is telling me something.

Greg's commentary continued on next page >

If it's been there the whole time, then there's potentially something seriously wrong with my operational patching.

If it's just popped up, do I have an issue with how new systems are built, or with how it's possible to install old, vulnerable software on existing systems? Maybe those processes are fine, but there's a procurement or shadow-IT issue bypassing them?

It's these issues in our processes that create the accumulation of risks that will contribute to an eventual breach. Addressing them drives cumulative and sustainable reductions in how much risk the business introduces over time, meaning we have less and less to worry about.

Finding these issues can be surprisingly easy: our vulnerabilities are telling us exactly where these issues are.

The vulnerabilities we've fixed in the past—without considering where they came from—may have been a missed opportunity to find the root cause of the very thing that gets us breached in the future.

Terry Cutler

Ethical Hacker & Founder, Cyology Labs

Protecting your business: advice from a professional hacker

The reality is that, whether you operate as a solo businessperson or manage a thriving enterprise, it's essential to recognize that cyber threats can target anyone. As cyber threats evolve in complexity, no entity remains immune. Recent trends reveal a significant uptick in incidents that impact local governments, municipalities, and businesses, and result in substantial financial losses.

How hackers operate: the insider's playbook

Hackers typically employ a structured attack approach that consistently involves a few phases. They start with reconnaissance, gathering digital information, similar to tracing breadcrumbs online. Next, they conduct scans to find vulnerabilities, like a burglar checking for unlocked doors.

Once they find an entry point, they move on to exploiting it to gain and maintain access, while covering their tracks. Finally, they systematically disrupt systems.

Terry's commentary continued on next page >

The game plan for cyber resilience

Implementing basic cybersecurity practices can prevent many attacks. Simple actions—like keeping your software updated, staying up to date with patches issued by Microsoft, being cautious of phishing scams, and using strong, unique passwords with two-step verification—are essential. As BeyondTrust's Microsoft Vulnerabilities Report has continually shown, removing unnecessary admin rights and achieving least privilege is a vital step in this process. It's like locking your doors and windows—simple, yet effective at keeping intruders out and only allowing access to the right person at the right time.

Conducting a comprehensive cyber assessment to uncover any vulnerabilities is crucial

To protect your network, endpoints, and cloud infrastructure effectively, adopt advanced strategies like multi-factor authentication (MFA), encryption, identity and access security, and modern cyber defence technologies. Customize your defences to your specific risks and be ready to adapt to keep up with evolving threats.

Sami Laiho

Windows OS MVP
Chief Research Officer / Founder, Adminize
LinkedIn
X (formerly Twitter)

As the 2024 Microsoft Vulnerabilities Report says, "total vulnerabilities continue their 3-year holding pattern near the highest-ever numbers." We stopped testing Anti-Malware Definition Updates before deploying them when there were less of them because we now have monthly Windows Updates. *Did they sometimes fail? Yes. Did we stop upgrading? No*. I think any one of us will choose a potential two-hour downtime that we are prepared for and in control of, rather than a three-month downtime controlled by a third party.

I have a rule with my customers: critical patches or patches for anything with a public IP will get patched on days 1-3. Everything else gets patched ASAP – and for your Firewalls and VPN gateways, you patch on all days that start with a letter T: Tuesday, Thursday, Today, and Tomorrow. With the principle of least privilege, we can still mitigate around half of all critical vulnerabilities, so it is still one of the immutable laws of Windows Security – like the NT 3.1 user guide from 1993 says, there is no security in Windows if you log in as an admin.

Luckily, Zero Trust (however bad a name it is) has raised the Principle of Least Privilege to most of our lips. Malicious actors need admin rights to run the really dangerous tools, so that is what they are after. As the Microsoft Vulnerabilities Report shows, "Elevation of Privilege accounted for 40% (490) of the total vulnerabilities in 2023."

> "Since privileges are what threat actors want, our main job should be to make sure they don't get them."
>
> **Sami Laiho, Windows OS MVP,**
> **Chief Research Officer / Founder, Truesec Finland**

Eliza-May Austin

CEO
th4ts3cur1ty.company

Vulnerability management, elevation privileges, and identity as an attack surface

We see from the results of the 2024 Microsoft Vulnerabilities Report that the Elevation of Privilege phase (PrivEsc) continues to dominate as a successful offensive tactic. PrivEsc, a necessary and required phase of attack, will become the focus for threat actors, even more than penetrating the perimeter.

The predictability of a structured perimeter in the classic sense is dwindling, with companies of all sizes aiming to reduce their classic architectures in favour of the "serverless" approach. User Identity will become the preferred attack surface, versus the traditional perimeter. Threat actors will attack the identity (the account) over system compromise, as companies become more aligned with zero trust as an architected approach. This means zero trust is, in theory, circumvented.

Concentration on the account holder will lead to an increase in the need for digital forensics and incident response (DFIR) structures and capabilities. It's crucial to acknowledge the vast amount of data collected by national adversaries. This could be cross-referenced against corporate data with personal information, enabling adversaries to pinpoint specific vulnerabilities in the account holder. This, in turn, facilitates highly targeted attacks on individuals' identities. Such attacks can effectively exploit the account holder's weaknesses to gain access where a zero day attack may have otherwise been required. It costs time, money, and human resources to develop custom, never-before-seen attacks (zero days), and if a threat group can avoid burning one (using it) by focusing on identities instead, then they will. They will always look to the lowest hanging fruit and attack users that make mistakes or systems that are not defended well.

Eliza-May's commentary continued on next page >

Attacking accounts will undoubtedly lead to more complex and, frankly, impressive supply chain attacks. We may even see this expand further, with attacks evolving to more distanced forms of attack, from supplier-to-supplier to supplier-to-target, and on and on. As the reliance on SaaS continues to grow in an attempt to circumvent this expansion, we will notice an increase in what I like to call 'Jackpotattacks,' like those of SolarWinds and FireEye.

Referring back to the Microsoft Vulnerabilities Report, it's crucial to prioritise vulnerability management and educate businesses on distinguishing between scanning and management. Acquiring scanning licenses is simple, but establishing an internal process to identify, prioritise, remediate, and test mitigations remains a consistent challenge, due to cross-departmental dependencies and a lack of KPIs measuring vulnerability exposure reduction.

Marc Maiffret

CTO
BeyondTrust

As CTO of BeyondTrust and a fan of Spinal Tap, I am excited to see this report turning it ***"up to eleven"*** this year. As well as being "one louder than ten" (I promise, no more Spinal Tap references), this report continues to highlight the need to keep improving security, not only at Microsoft, but also for all organizations who are looking to better manage cyber risks in the context of an evolving threat landscape.

While the number of critical Microsoft vulnerabilities is hitting all-time lows, there are some good examples in the report of reasons not to become complacent when it comes to vulnerabilities. Despite major strides forward in the overall security of the Microsoft ecosystem, CVE-2023-23397 allowing NTLM hashes to be captured via Outlook, and CVE-2023-36884 allowing for Mark of the Web bypasses, both show us that there are still plenty of attack surfaces out there just waiting to be found and exploited.

The continued domination of Elevation of Privilege as the most common category of vulnerability, and the identity crisis highlighted at the end of the report, highlight the importance of privilege and the timeless security concept of least privilege.

Marc's commentary continued on next page >

Early in my career, I was fortunate to be introduced to the Rainbow Books, a series of computer security standards published by the U.S. Department of Defense in the 1980s and 1990s. These books, and the concepts of attack surface and least privilege described in them, are just as relevant to the challenges we are seeing today as they were over 30 years ago, when the books were first published.

> "Least privilege - this principle requires that each subject in a system be granted the most restrictive set of privileges needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use."
>
> **A Guide To Understanding Discretionary Access Control In Trusted Systems, 1987**

When I think about identity security today, it isn't the identities themselves that have value, it's the privileges those identities can access that have value and make them a target. This is why threat actors seek out elevation of privilege vulnerabilities and identities with access to privileges. This is why patching and least privilege remain some of the best ways to reduce your attack surface. It is also why BeyondTrust is on a mission to provide the broadest level of visibility and protection of privileges.

The Midnight Blizzard attack referenced in this year's report was a prime illustration of the modern identity threat landscape. With that in mind, I'm going to throw down a challenge to the authors of this report for next year to go beyond Microsoft software vulnerabilities and analyze some of the common misconfiguration or weak default settings that introduce configuration vulnerabilities into the Microsoft ecosystem, allowing attackers to access privileges and exploit systems.

Stay safe!

Dr Jessica Barker MBE

Co-Founder, Cygenta
Author of Hacked: The Secrets Behind Cyber Attacks
LinkedIn
X (formerly Twitter)

The data this year continues to show that putting in the work in security does pay off. Working in this field, it can sometimes feel like we make no progress, or even that we're moving backwards—that attackers win so much more often than we do.

We have to look for the flaws—the one time something goes wrong rather than the 100 times it goes right. And with an ever-evolving threat landscape, it can feel like we're swimming against the tide.

This is why we must look at the bigger picture, recognising that the complex problems of cybersecurity won't be solved overnight, and taking stock of progress that we make along the way.

It is no surprise that escalation of privilege remains the number one category of vulnerability in this year's report. But even this, the number one category of vulnerability, shows marked improvement. This serves as a reminder that we can't fix everything overnight, but we can make progress, even in challenging areas.

This year's report highlights that attackers "think in graphs". In cybersecurity, we need to think in systems, too. When it comes to social engineering and the human side of security, it can be easy to focus on so-called human error. However, if we focus solely on the individual, we miss the mark.

Instead, we need to look at the systems in which people operate, reducing the burden for end users. Segmented networks, least privilege, multi-factor authentication, and vulnerability management are foundational, underpinned by a healthy security culture.

This report also highlights the importance of identity. With the rise of generative AI and deepfake technology being used in social engineering attacks, identity management is going to become an even more pressing issue. It is more crucial than ever that we raise awareness of threats, while doing everything we can to reduce security friction, empowering people to practice secure behaviours within a positive and proactive security culture.

Mitigating Microsoft Software Ecosystem Risks & Enhancing Cyber Resilience

Together, the following security strategies provide highly effective defense-in-depth protection against Microsoft vulnerability exploits and also identity-based attacks:

1. **Enforce least privilege by removing local admin rights:** It is essential to maintain a robust Privileged Access Management strategy to remove and secure privileges within an environment to prevent them from falling into the hands of an attacker. This proactive approach can provide highly effective protection, even in the absence of patching. Removing local admin rights and controlling execution has historically mitigated 75% of Microsoft's critical vulnerabilities, as we have demonstrated in past reports when Microsoft made more privilege-specific data available. This 75% stat indicates that, without admin rights, the vulnerability cannot be exploited—even if it remains unpatched. A least privilege approach, which is also a core tenet of zero trust security models, can help break multiple points in the attack chain – from account hijacking to lateral movement, to privilege escalation, and more.
2. **Follow security hardening protocols, such as patching:** Always ensure your operating system and third-party software are up-to-date and you are not using end-of-life software in your environment. In addition, remove unneeded privileges, access, and accounts to further reduce the risk surface. Keep in mind that patching sooner rather than later can also help you prevent a seemingly innocuous vulnerability from snowballing into a bigger threat.
3. **Secure remote access pathways:** Microsoft's Remote Desktop Protocol (RDP), as well as VPNs and many other common remote access technologies, are increasingly stretched beyond their proper use cases, resulting in security exposures and breaches. Ransomware often uses RDP as an entry point. Ensure RDP is not exposed to the internet. Do not allow VPNs and BYOD to mix. Replace VPNs or augment them with zero trust security controls for vendor access and privileged access use cases.
4. **Tailor vulnerability management to your own environment:** It is critical to find, prioritize, and determine a remediation path for all vulnerabilities. Without the context of your own organization's threat models, you can't fully understand how best to prioritize patches and/or use other security hardening controls and mitigations. What is considered a critical patch for one organization may not be so for another. Leverage your business context to create the vulnerability management strategy that best addresses your risks.
5. **Stay vigilant to emerging threats:** Understanding threats goes a long way toward making more informed decisions and keeping yourself secure. The past decade has ushered in considerable changes to the Microsoft threat landscape. With the rapid development and deployment of AI technologies, we are likely to see many impactful shifts in threats over the next decade and beyond.
6. **Implement identity threat detection and response (ITDR):** Organizations need to make proactive security posture changes and corrections to prevent threats from gaining a foothold, and they also need to orchestrate a rapid response to any attacks that do rear their head. ITDR, or essentially identity defense-in-depth, is a multi-discipline approach that aims to integrate capabilities for holistic identity security visibility, threat detection, investigation, and response capabilities. This begins with complete visibility into the identity security posture across all enterprise identity stores (Active Directory, Entra ID, Okta, Ping, and more). From there, organizations can gain understanding of the attack paths that can operate through those identities, and what steps are needed to improve posture or break an attack.

How BeyondTrust Mitigates Traditional Vulnerabilities & Modern Identity-Based Risks

BeyondTrust combines complete privileged access management, along with CIEM and ITDR capabilities, to mitigate Microsoft vulnerabilities and protect the entire identity infrastructure—from Active Directory to Entra ID and beyond.

Customers rely on BeyondTrust solutions to:

- Remove admin rights and implement a true least privilege model consistent with zero trust principles.
- Secure remote access pathways and infrastructure by ensuring all access by employees, vendors, and others is granularly controlled and audited.
- Prevent account hijacking and privilege escalation by securely managing all human and machine privileged credentials, DevOps secrets, SSH keys, and employee workforce passwords that touch the enterprise.
- Manage, monitor, and audit every privileged session—no matter how ephemeral.
- Effectively manage and reduce the entire identity attack surface, spanning Microsoft and other identity stores (Okta, Ping, etc.).
- Intelligently detect and neutralize identity attacks with velocity and precision.
- Satisfy rigorous compliance and forensic requirements by providing easy-to-access reporting on all privileged activity and other identity insights.
- Qualify for cyber insurance by meeting several key security controls demanded by cyber insurance providers and policy underwriters.

With BeyondTrust, organizations get the best of both worlds—the most advanced proactive protection against external threats (ransomware, malware, etc.) and insider threats, along with detection and response capabilities to stop in-progress attacks. **Learn more.**

> "Long-lived privileged credentials show up in so many breach reports, We have to manage these better and eliminate them where we can."
>
> **Jay Beale, CEO, CTO, InGuardians, Inc.**

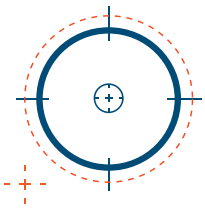
Conclusion

While total Microsoft vulnerabilities remain just off their all-time highs, they have more or less plateaued since 2020. During this same time period, the number of critical vulnerabilities has continued its downward trend.

The stabilization in the overall number of vulnerabilities reflects the substantive security investments and focus on the part of Microsoft. Yet, as some eyebrow-raising critical vulnerabilities and innovative new threat tactics leveraged this past year have shown, now is not the time to get complacent. There are numerous vulnerabilities to go around, including unpatched systems with known vulnerabilities that make it all too easy for threat actors to launch a successful attack.

Moreover, as the Microsoft technology estate continues to expand, it will bring with it new attack surfaces and potential threat vectors. Vulnerabilities will also continue to emerge in ways that have never been seen before, and threat actors will continue to think in graphs to navigate innovative pathways through Microsoft's systems.

As we have shown in the 11 years this report has been running, the Microsoft vulnerability landscape is constantly evolving. While vulnerabilities remain a significant part of the attack surface, investments in research and security practices are increasingly forcing threat actors to innovate. This will continue to shift the way threat actors gain their foothold within victim environments.



We are fast reaching a remarkable tipping point where it is becoming easier for threat actors to steal an identity to gain access than to exploit a vulnerability.

This means we can expect to see the volume and sophistication of identity-based attacks increase considerably as threat actors focus on identities as a much more fruitful means of attack.

One piece of favorable news for defenders is that the long-standing, foundational security principles that have been tried and tested for the past decade continue to offer the best line of defense—even against modern threats.

Least privilege is critical for reducing all attack surfaces across endpoints and identities. The fewer privileges the victim has, the lower the risk of account compromise—even during zero-day exploits—and even when an attacker reverse engineers a patch to find an exploitable workaround.

Those organizations who successfully pair preventative security controls with threat detection and response will continue to be much better poised to withstand tomorrow's threats. And as always, we'll continue to offer our insights to help our readers stay alert to the latest threats, the most impactful vulnerabilities, and the most effective strategies to strengthen their security posture.

Methodology

On the second Tuesday of every month (known as "Patch Tuesday"), Microsoft releases security bulletins announcing fixes for any vulnerabilities affecting Microsoft products.

The annual BeyondTrust Microsoft Vulnerabilities Report compiles these releases into a year-long overview and analyzes the data, creating a holistic view of trends related to vulnerabilities.

Until November 2020, Microsoft had been using their own method of sharing CVE details via their Security Update Guide.

The former Microsoft reporting format featured an executive summary for each reported vulnerability that would include the following verbiage:

- Customers/users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.
- If the current user is logged on with administrative user rights, an attacker could take control of an affected system.

From this summary, security researchers could deduce whether any given vulnerability (specifically, the critical ones) could have been mitigated had admin rights been removed from the user.

In 2021, Microsoft shifted methodologies and moved to the Common Vulnerability Scoring System (CVSS). And in 2023, Microsoft continued to use CVSS 3.1 scoring for their vulnerabilities, but began ranking severities based on Microsoft's own Security Update Severity Rating System.

The CVSS methodology allows Microsoft's vulnerabilities to be cross-referenced more easily with third-party bugs, simplifying some analysis, and Microsoft's Security Update Severity Rating System allows each vulnerability to be rated according to the worst theoretical outcome, should that vulnerability be exploited.

An unfortunate trade-off of this change, however, was the loss of the ability to determine the impact of admin rights on critical vulnerabilities.

Not only do the risks of excess privileged access remain very much intact, but privileged attack vectors are rapidly growing with the expansion of the cloud, and the proliferation of human and machine identities and accounts.

Thus, while the statistics on admin rights may be absent from this year's report, it's imperative that organizations don't get complacent. Removal of admin rights remains a key piece of a least privilege strategy, as well as for enabling zero trust.

Accuracy of Vulnerability Data

A number of generalizations have been made for each vulnerability, as follows:

- Each vulnerability was classified with the highest severity rating of all instances of that vulnerability where it appeared multiple times.
- Each vulnerability was classified with the most prevalent type for all instances of that vulnerability.
- Product versions were not taken into account.
- Product combinations were not taken into account.
- Vulnerabilities were counted for both the software and version where appropriate (for example, a vulnerability for Microsoft Edge on Windows 10 is taken as a vulnerability for both Microsoft Edge and Windows).

>>> Additional Resources

ASSESSMENT	**Gain Control Over Your Entire Identity Attacks Surface**. Start with a free identity security assessment and monitoring of your IT estate to illuminate excess privileges, misconfigurations (lack of MFA, etc.), orphaned accounts, in-progress attacks, and much more. Also gain clear intelligence on threat context and remediation steps.
TEST/ CHECKLIST	**Need a VPN Alternative?** Take the Remote Access Test: Learn if your team has the appropriate secure remote access tools in place to handle the large volume of users who are connecting remotely into your network.
CHECKLIST	**Cybersecurity Insurance Checklist:** Leverage our checklist to see how well your organization complies with the stringent underwriting requirements needed to qualify for cyber insurance.
SOLUTION GUIDE	**A Guide to Endpoint Privilege Management:** Learn how endpoint privilege management (EPM) combines least privilege with application control to significantly reduce the attack surface across Windows, macOS, and Linux.
WHITEPAPER	**Buyer's Guide for Complete Privileged Access Management (PAM):** Understand the must-have PAM capabilities necessary to properly secure identities and access across your environment, eliminate and mitigate many threat vectors, and help you advance along your PAM journey.
BLOG	**Shelter from the Storm – What Midnight Blizzard's Attack on Microsoft Tells Us about Modern Identity-Based Attacks:** Discover the unique features that set this attack apart and learn why this nation-state attack against Microsoft highlights the importance of an identity-first approach to security.

About BeyondTrust

BeyondTrust is the worldwide leader in intelligent identity and access security, enabling organizations to protect identities, stop threats, and deliver dynamic access. We offer the only platform with both intelligent identity threat detection and a privilege control plane that delivers zero-trust based least privilege to shrink your attack surface and eliminate security blind spots.

BeyondTrust protects identities, access, and endpoints across your organization, while creating a superior customer experience and operational efficiencies. We are leading the charge in innovating identity-first security and are trusted by 20,000 customers, including 75 of the Fortune 100, plus a global ecosystem of partners. Learn more at **www.beyondtrust.com.**