



> See into the past, present, and future of the Microsoft vulnerability landscape

2023 Microsoft Vulnerabilities Report

A Decade of Vulnerability Insights
to Help Organizations Everywhere
Improve Cyber Defenses

ANNIVERSARY
EDITION





TABLE OF CONTENTS

Executive Summary	3
Key Findings & Data Highlights	4
Microsoft Across the Decade	5
Understanding Critical Vulnerabilities	8
Report Retrospective	11
Vulnerabilities Data Deep-Dive	14
The Vulnerability Snowball Effect	26
What Does ChatGPT Say?	28
What Do the Experts Say?	31
Mitigating Microsoft-Based Vulnerability Risks	39
Conclusion	41
Methodology	42
Additional Resources	43



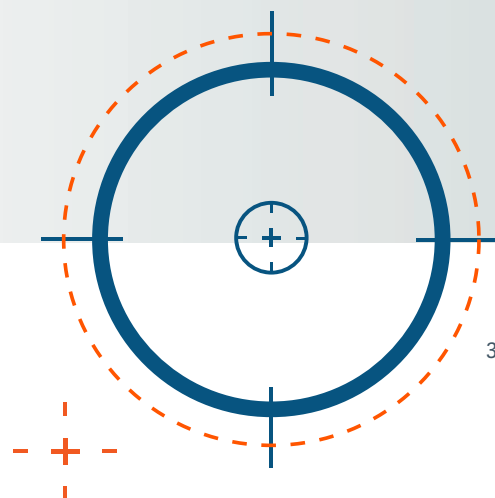
The Microsoft Vulnerabilities Report is proudly celebrating its tenth year.

Since the report debuted in 2013, it has garnered over 15,000 downloads and has benefited thousands of users with detailed data analysis and expert findings.

This 10-year anniversary edition of the report dissects the 2022 Microsoft vulnerabilities data and highlights some of the key shifts since the inaugural report. This report will spotlight some of the most significant CVEs of 2022 (9.0+ CVSS severity scores), break down how they are leveraged by attackers, and explain how they can be prevented or mitigated.

A panel of some of the world’s leading cybersecurity experts will weigh in on the report findings. We will also have a special AI guest weigh in as we look ahead to how the next decade of threats, vulnerabilities, and cyber defenses may unfold.

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





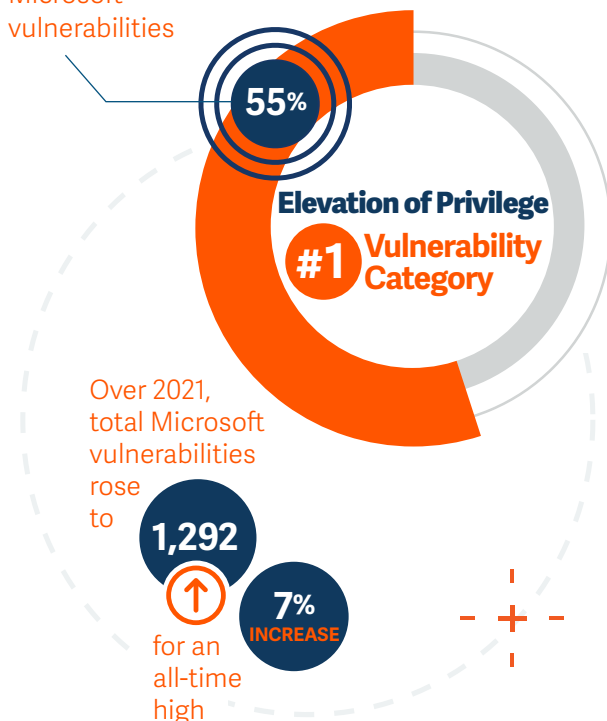
Key Findings & Data Highlights

In 2022, total Microsoft **vulnerabilities rose to 1,292, hitting an all-time high** since the report began 10 years ago.

However, it's not just the number of vulnerabilities that should be of concern, **but also the unique threat and impact** posed by individual vulnerabilities.

- 1 The **Elevation of Privilege category dominates** the Microsoft vulnerability landscape for the third year in a row and continues its rise.
- 2 Microsoft Azure and Dynamics 365 are not only generating the biggest financial gains for Microsoft; they are also **propelling the biggest gains in number of vulnerabilities.**

Elevation of Privilege accounts for **55% of the total** Microsoft vulnerabilities



Critical vulnerabilities dropped for the 2nd year in a row, **hitting a five-year low of 89 in 2022.**

In 2022, 6.9% of Microsoft's vulnerabilities were rated as 'critical,' while in 2013, 44% of all Microsoft vulnerabilities were classified as 'critical.'

Azure & Dynamics 365 vulnerabilities skyrocketed by 159%, from 44 in 2021 to 114 in 2022.

Microsoft Edge experienced 311 vulnerabilities last year, but **none were critical.**

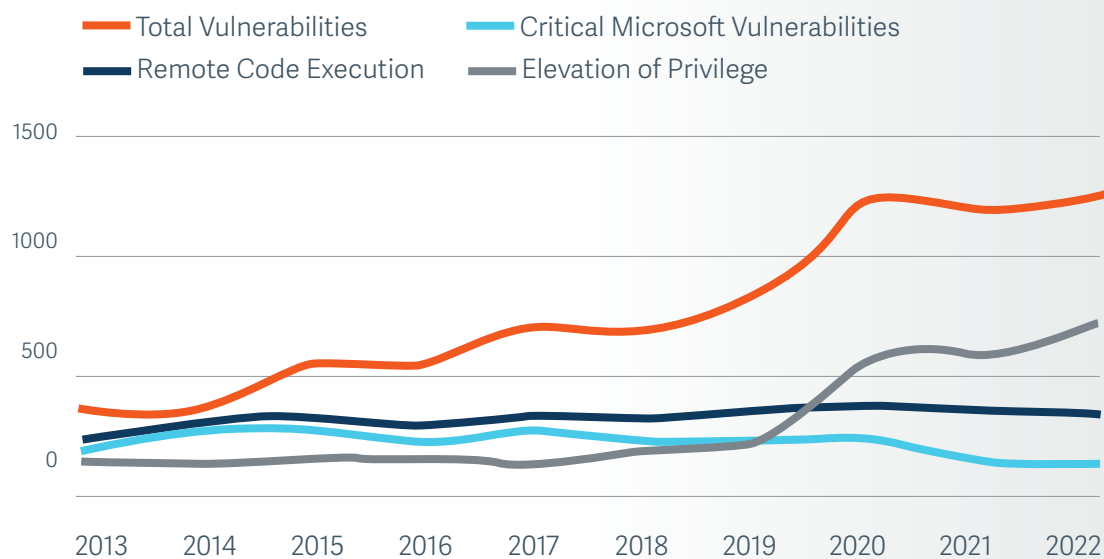
There were **513 Windows vulnerabilities in 2022**, 49 of which were critical.

Microsoft Office experienced a **five-year low of just 36** vulnerabilities in 2022.

Windows Server vulnerabilities rose slightly to 552 in 2022.



A Snapshot of Microsoft Across the Decade (2013 – 2022)





Microsoft: Then & Now

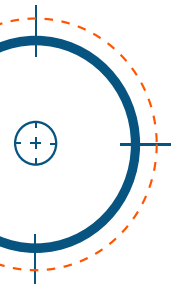
	2013	2022
Market Capitalization (in USD, as of December 31)	\$314 Billion	\$1.79 Trillion
Number of Global Microsoft Customers (2013 data for FY2013; 2022 data accurate as of October 24, 2022)	1.5 billion Windows users around the world More than 1 million Office 365 Home Premium subscribers	1.4 billion monthly active devices running Windows 10/11 60 million Microsoft 365 consumer subscriptions; 25 million monthly active users on Power Platform; 270 million monthly active users on Teams
Microsoft CEO	Steve Ballmer	Satya Nadella
Top Product Launched (based on % revenue increase within the fiscal year)	Office 2013 Windows 8.1	Windows 11 Windows Server 2022 Datacenter: Azure Edition SQL Server 2022
Top Acquisition	Nokia (\$7.2 billion USD)	Activision (the \$70 billion USD acquisition was the biggest acquisition ever in the gaming industry & largest-ever acquisition by Microsoft)
Products Accounting for Largest Share of Microsoft Revenue	Office products (\$23 billion USD in FY2013)	Server products and cloud services (\$67.3 billion USD in FY 2022)
Intelligent Cloud Revenue	\$15.4 billion USD (classified as Server Products & Cloud Services Revenue)	\$65.29 billion USD
Mantra	2013 added “creating a family of devices” into its mission statement and sparked the “One Microsoft” vision	“Intelligent Cloud” was announced May 2017, supplanting “Mobile First, Cloud First”, which was announced May 2014
How Security & Privacy is Structured at Microsoft	Trustworthy Computing Unit (TwC) centralized privacy and security practices across Microsoft	Security and privacy responsibilities are embedded across the business (TwC was broken up in 2014)
Microsoft’s Vulnerability Reporting Methodology	Sharing CVE details via Microsoft’s Security Update Guide	CVSS standard (adopted November 2020). Change to CVSS enabled simplified cross-referencing with third-party bugs, but the reporting change also meant the impact of admin rights on critical vulnerabilities could not be clearly determined.
Total Number of Microsoft Vulnerabilities	333	1,292



	2013	2022
Total Number of Critical Microsoft Vulnerabilities	147	89
#1 Microsoft Vulnerability Category	Remote Code Execution	Elevation of Privilege
Product Areas with the Most Vulnerabilities	Microsoft Windows Server (252) Windows XP, Vista, Windows 7 and Windows 8 operating systems (252)	Microsoft Windows Server (552), Microsoft Windows (513), Microsoft Edge (311), Azure & Dynamics 365 (114)
Recurring Vulnerabilities (Vulnerabilities that reoccur or take years to fully resolve, in this case spanning the 10-year duration of this report)	CVE-2013-3900 (A remote code execution vulnerability caused when the WinVerifyTrust function improperly validates the file digest of a specially crafted PE file while verifying a Windows Authenticode signature)	The 2013 vulnerability was republished by Microsoft in 2022 to notify customers that an update to Windows 10/11 addresses it

So, what hasn't changed?

- The need for an effective vulnerability management program (finding, prioritizing, and remediating vulnerabilities)
- The need for removal of admin rights and enforcement of least privilege to proactively mitigate vulnerabilities





Understanding Microsoft Critical Vulnerabilities

While the total number of vulnerabilities is an important metric for gauging the health of an environment, as we will cover in this report, vulnerabilities are not created equal.

Some vulnerabilities may pose mostly theoretical risk (low likelihood) and low impact if they are exploited, while 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).

Measurement of a vulnerability's impact will relate to its impact to 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 as, generally speaking, attackers are far 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 a user being socially-engineered.

→ **These are the types of vulnerabilities that keep IT admins awake at night and pose the most risk and challenges to businesses.**



How does Microsoft classify critical vulnerabilities?

The [National Vulnerabilities Database \(NVD\)](#) classifies critical vulnerabilities as those given 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 only 22 Microsoft vulnerabilities from 2022 scored a nine or above (making them “critical” under the National Vulnerability Database scoring system), Microsoft has classified 89 of its vulnerabilities as critical.**

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

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 unavoidable 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.

Microsoft’s severity rating system may offer better insights for prioritization of risk reduction.



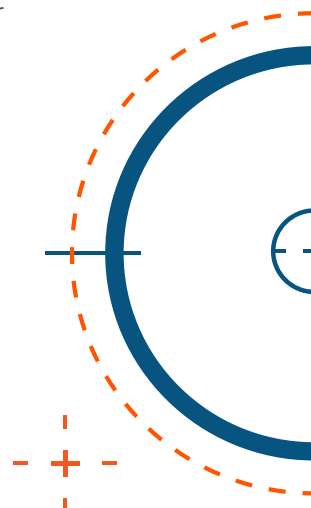
The difference between CVSS scoring and Microsoft's severity rating system is worth noting, not only when considering the data in this report, but also when considering risk in your organization. **CVSS scores measure the technical severity of a vulnerability.**

For example, 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 of the data provided by Microsoft's severity rating system is based on the information that was available at the time, and 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 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.



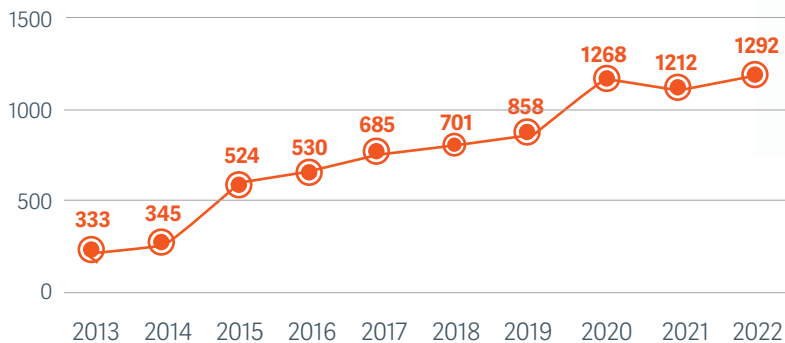


Report Retrospective

A Ten-Year Summary

Here's how this year's Microsoft vulnerability findings align to the 10-year trends.

Total Number of Microsoft Vulnerabilities (2013 - 2022)



Total number of Microsoft vulnerabilities hit an all-time high, but are they levelling out over the long-term?

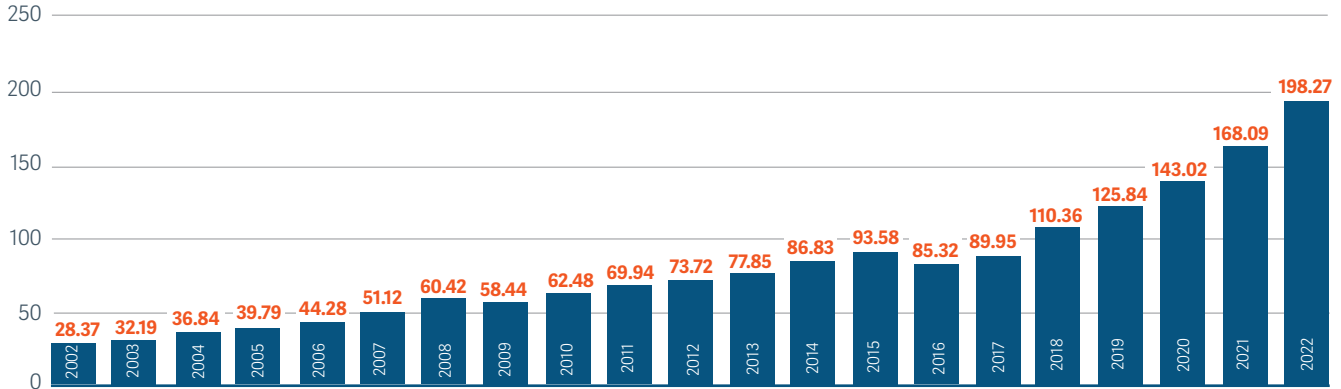
2022 set a new high for the number of Microsoft vulnerabilities, edging ahead of the previous highwater mark set in 2020 by 2%. However, if we look at the longer-term trend, we can see that the number of vulnerabilities appears to be plateauing a little after years of significant growth.

Why are we seeing this pattern? To quote The Notorious B.I.G., “Mo Money Mo Problems,” and this appears to be very much the case for Microsoft. To increase their revenue, they create new products and improve existing ones. At the same time, these new offerings potentially increase the attack surface by providing new code.

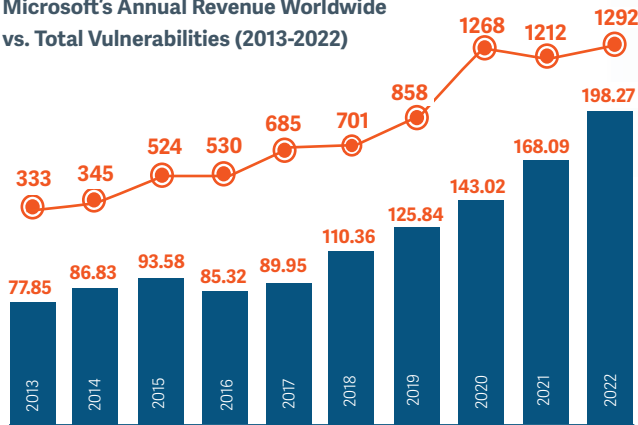
In addition, the more customers you have, the more people are looking at your software—from internal research teams to external pen testers, as well as ill-bent nation states and cyber criminals.



Microsoft's Annual Revenue Worldwide from FY 2002 to FY 2022 (in Billion USD)



Microsoft's Annual Revenue Worldwide vs. Total Vulnerabilities (2013-2022)



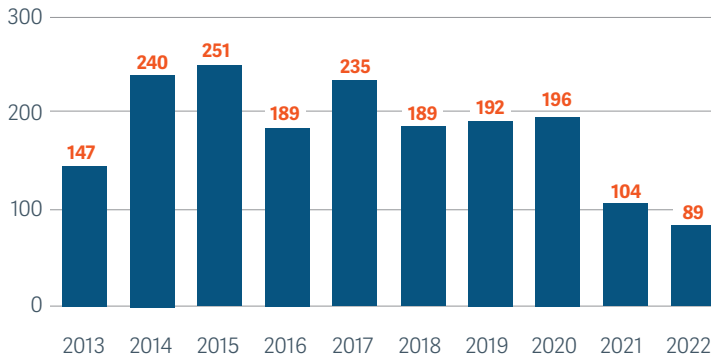
Microsoft's total revenue and total vulnerabilities both doubled between 2017 and 2020

So, does "Mo Money" really cause "Mo Problems?" While this isn't an exact measure, if we look at Microsoft's total revenue from 2013 to 2022 and compare that with the total number of Microsoft vulnerabilities, we can see a similar trend, with both revenue and vulnerabilities almost doubling between 2017 and 2020.

Moreover, if we drill down into the product areas with the biggest growth, we see Microsoft Azure and Dynamics 365 not only making the biggest financial gains for the company (cloud revenue accounted for 51.4% of Microsoft's total revenue in 2022), but also representing the largest gain in vulnerabilities, as represented by both the increase in number of vulnerabilities (70) and the percentage increased (159%) in 2022.



Microsoft Critical Vulnerabilities (2013 - 2022)



The number of critical Microsoft vulnerabilities reached their lowest point across the 10 years of this report.

Critical Microsoft vulnerabilities dropped 55% since 2020, indicating a decrease in the overall level of risk associated with individual vulnerabilities.

In this 10th year of the Microsoft Vulnerabilities Report, we saw two records set for vulnerabilities that seem to highlight opposing trends.

While the total number of Microsoft vulnerabilities reached its highest recorded number in 2022, the number of critical vulnerabilities hit their lowest number, with less than half the number of critical vulnerabilities appearing in 2022 than we saw in 2020. In 2022, only 6.9% of Microsoft's vulnerabilities were rated as 'critical,' while in 2013, a substantial 44% of all Microsoft vulnerabilities were classified as 'critical.'

This trend indicates that, while overall vulnerabilities have increased in number, the risks and worst-case scenarios associated with these individual vulnerabilities have decreased from previous years. This also indicates that, while the overall Microsoft attack surface is expanding along with the expansion of Microsoft's business, the organization is doing a better job at minimizing the most dangerous types of development errors.

Microsoft has made significant investments in security improvements over the years, and we believe this is reflected in the downward trend in the number of critical Microsoft vulnerabilities. Many of Microsoft's products have had a very long tail of support, which means these security improvements are happening as organizations transition to more up-to-date and secure products, as well as to more SaaS instances, where everyone is kept on the latest version.



As critical vulnerabilities become scarcer, attackers may need to chain multiple, less severe exploits together to gain code execution, elevate privileges, and move around the network.

From a defender's point of view, this is a good thing because it requires a higher level of attacker skill and reduces the number of possible adversaries. It also provides more potential points to detect, intercept, and mitigate a breach.

If an attacker needs to chain three or more vulnerabilities together to reach their objective, then you just need to have mitigated or patched one of them to break the chain.



Vulnerabilities Data Deep-Dive

Remote Code Execution and Elevation of Privilege remain the top vulnerability categories.

Vulnerabilities by Category



Each Microsoft Security Bulletin is comprised of one or more vulnerabilities, applying 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 (DoS), Spoofing, Tampering, and Security Feature Bypass.**

In 2022, Elevation of Privilege and Remote Code Execution continued to tower over the other vulnerability categories.

With that aside, Elevation of Privilege vulnerabilities continue their strong growth trajectory, while Remote Code Execution vulnerabilities have been declining slightly over the past three years.

Elevation of Privilege vulnerabilities skyrocketed to 715 in 2022, a 22% increase over 2021, and a whopping 689% increase since 2017.

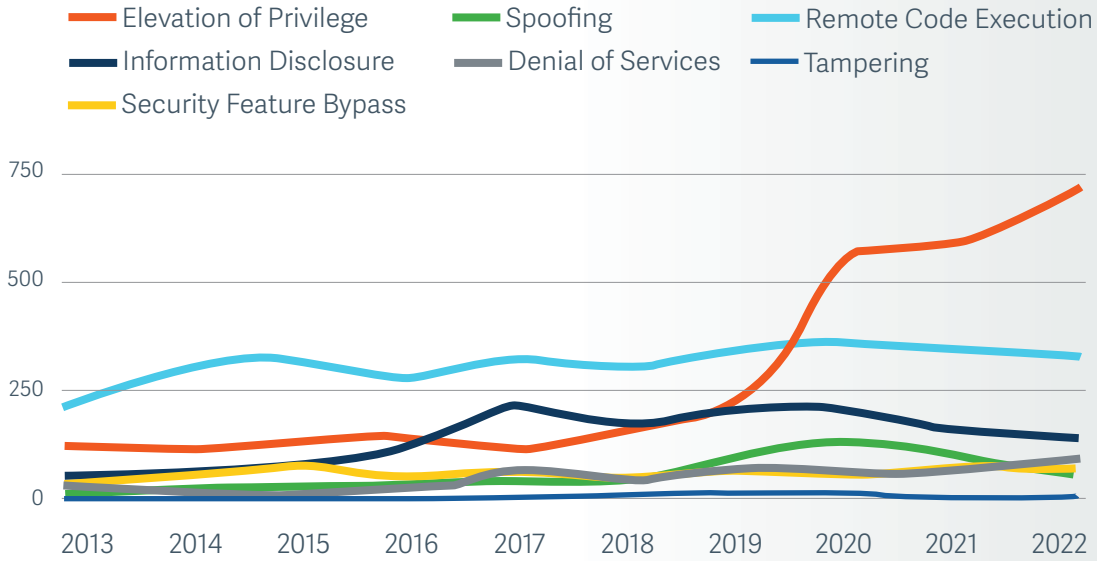
Remote Code Execution continued its slight downward trend following its 2020 peak, declining 4% in 2022 after falling 5.5% in 2021.

Microsoft Vulnerability Categories (2013-2022)

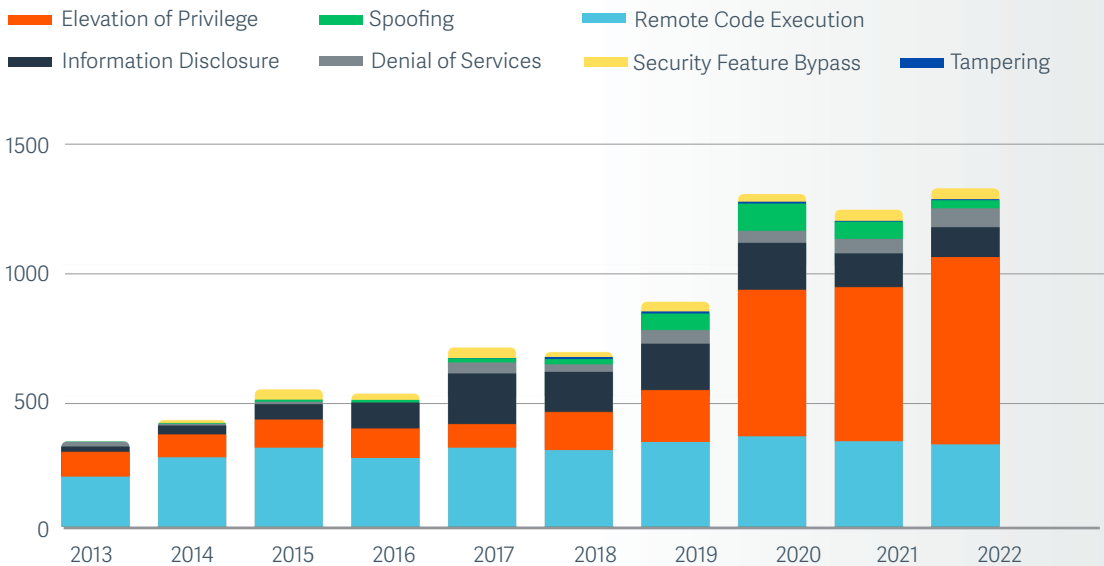
	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Remote Code Execution	190	264	301	262	301	292	323	345	326	314
Elevation of Privilege	95	87	107	112	90	145	198	559	588	715
Information Disclosure	20	34	59	99	193	153	177	179	129	114
Denial of Service	18	7	9	0	43	29	52	46	55	72
Spoofing	2	3	8	10	16	20	63	104	66	31
Tampering	0	0	0	0	1	8	8	7	3	4
Security Feature Bypass	0	12	40	25	41	20	38	30	44	42



Microsoft Vulnerability Categories (2013-2022)

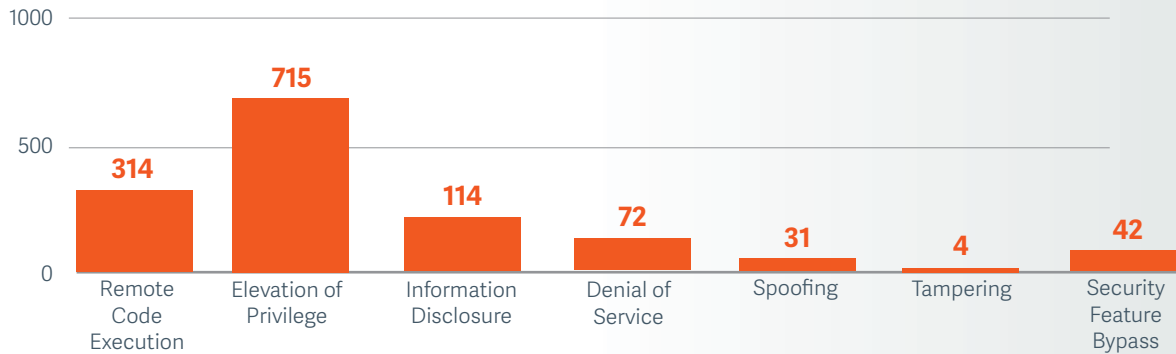


Microsoft Vulnerability Categories (2013-2022)





Breakdown of Microsoft Vulnerability Categories (2022)



What are the vulnerability categories telling us?

Vulnerability levels may be changing, but hackers' objectives remain the same, keeping emphasis on Remote Code Execution and Elevation of Privilege.

As we discussed above, having fewer critical vulnerabilities means attackers have fewer easy paths to totally compromise a system in one move. This is good news for organizations; however, an attacker's objective remains unchanged: they want to get their code to run, and they want it to be able to run with enough privileges that they can execute their malicious intent.

To achieve this objective, attackers need to have Remote Code Execution, the ability to launch their code on a target system, and Elevation of Privilege to make sure this code runs with enough privilege. This is reflected in the finding that Remote Code Execution and Elevation of Privilege remain the highest Microsoft vulnerability categories, as highlighted in this report. In particular, the number of Elevation of Privilege vulnerabilities across the Microsoft environment has been on a steep upward trajectory over the past three years.

The data from this report reflects that, as of 2022, Microsoft is making continued progress at reducing the number of critical vulnerabilities and removing excessive privileges, especially on endpoints. This is driving the need for attackers to exploit Elevation of Privilege vulnerabilities to succeed.



2 Key Security Takeaways from the Vulnerability Category Data

1

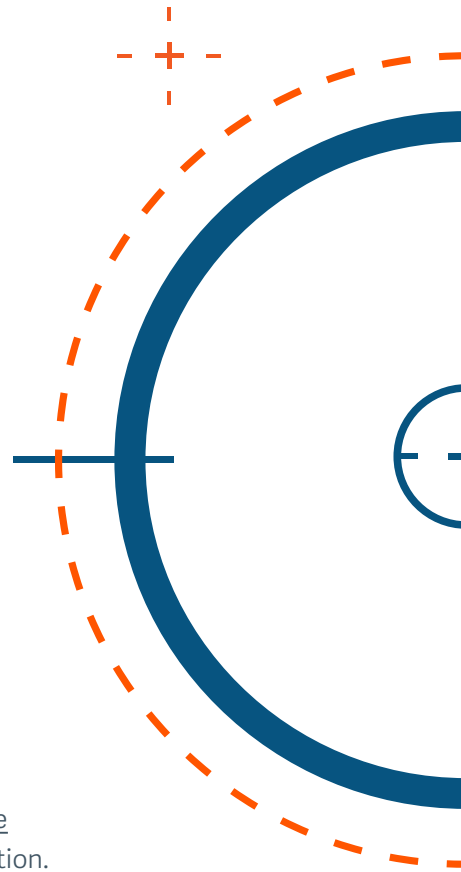
Always ensure your operating system and third-party software are up-to-date and you are not using end-of-life software in your environment.

2

Always ensure you are removing excessive privileges, especially on endpoints.

Unsurprisingly, the [SANS Institute's CIS Controls](#), the Australian Cyber Security Centre (ACSC)'s [Essential 8 Cyber Risk Controls](#), and [NIST's \(SP 800-207\) Zero Trust Architecture](#) also highlight these as essential cybersecurity controls for threat prevention and mitigation.

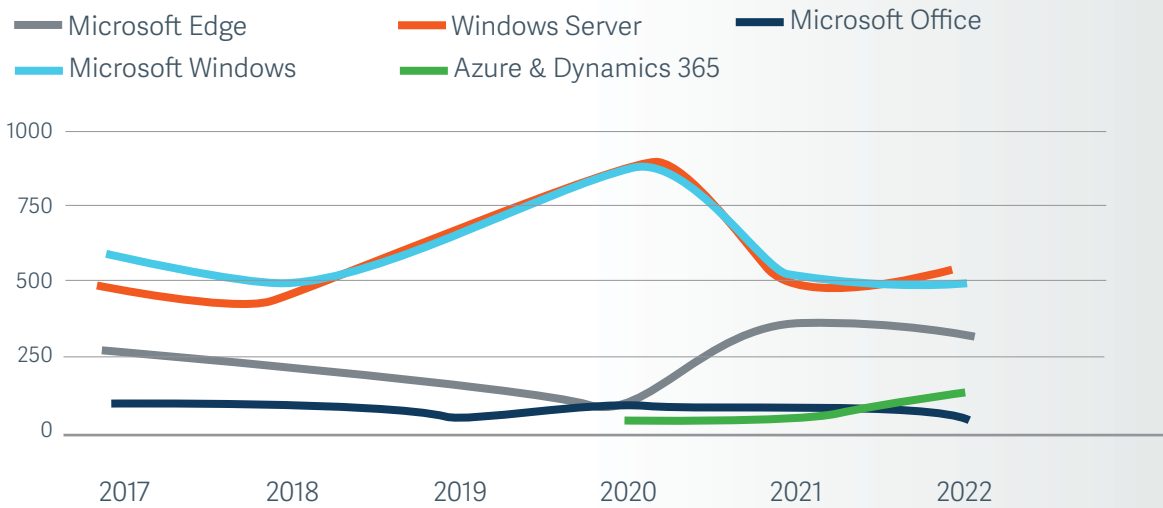
See our section on “Mitigating Microsoft-Based Vulnerability Risks” at the end of this report for more in-depth insights.



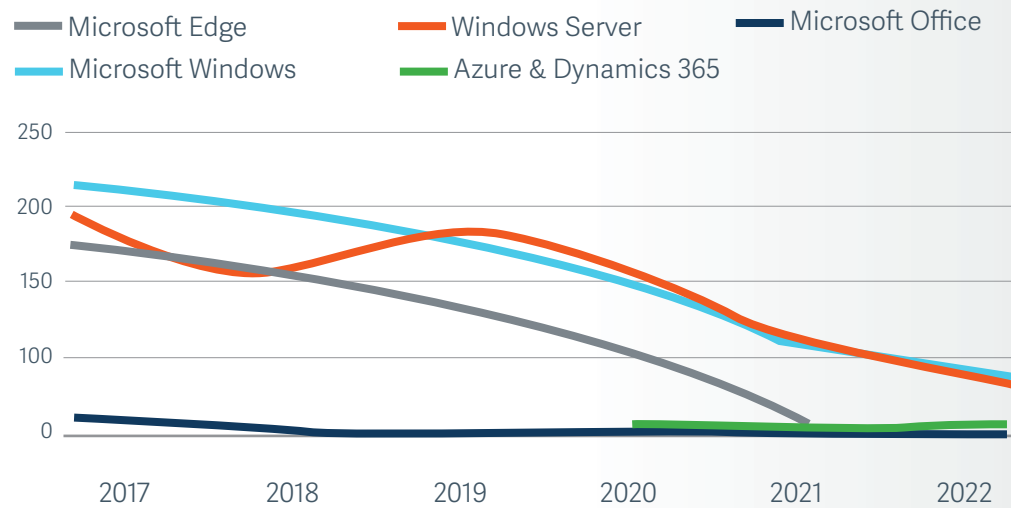


Vulnerabilities by Product

Vulnerabilities by Product (2017-2022)



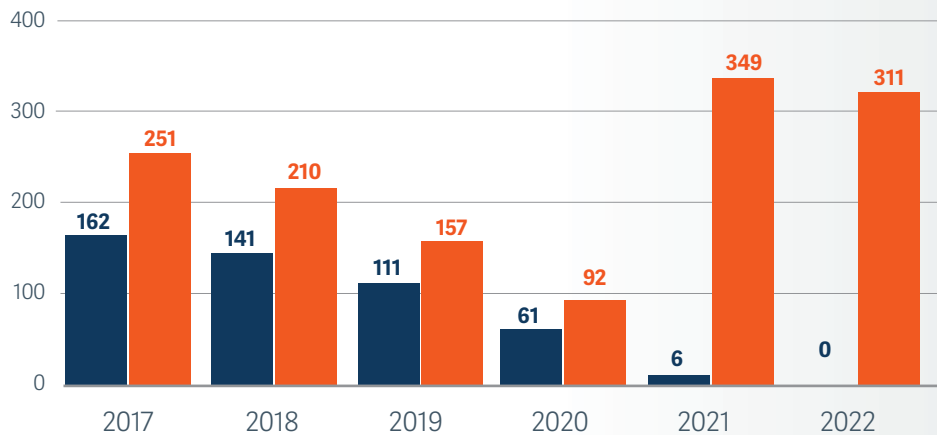
Critical Vulnerabilities by Product (2017-2022)





Microsoft Edge Vulnerabilities* (2017-2022)

■ Total Vulnerabilities
■ Critical Vulnerabilities



2017-2021 includes Internet Explorer, which was discontinued last year. 2022 figures are for Edge only.

After a nearly four-fold spike in 2021, Microsoft Edge total vulnerabilities decreased by 11%, to 311 vulnerabilities in 2022; critical vulnerabilities continue to plummet

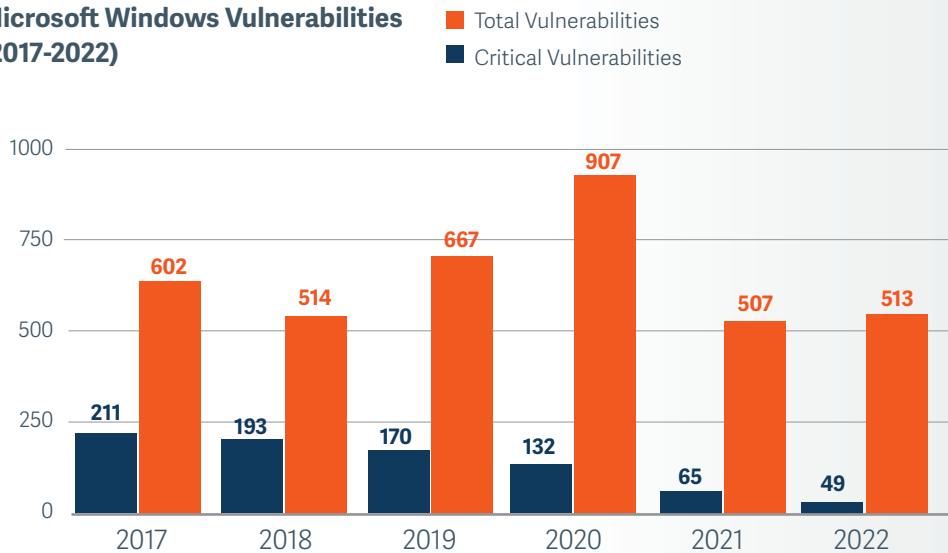
Those who are not familiar with what happened under the hood of Edge in recent years may be wondering what on Earth happened in 2020, when critical vulnerabilities suddenly plummeted and total vulnerabilities rocketed. This was when Microsoft ditched their own in-house browser engine and rebuilt Edge around Chromium. The benefits of this move were that, going forward, Microsoft could leverage the more mature and open source Chromium engine to resolve their critical vulnerability challenges, as well as a range of compatibility issues that often drove customers to only use Edge once—to download the Chrome installer.

The Chromium project benefits from being open source and ubiquitous enough to attract a lot of focus from the security research community. This focus has allowed it to rapidly mature. While other browsers may have a lower overall vulnerability count than Edge (or Chrome), this does not necessarily make them more secure.

The Edge vulnerability trends are a good example of what happens when there is no easy path for an attacker. A critical vulnerability in a browser may allow an attacker to gain privileged execution on a system just by having the victim click a malicious link. However, with no easy path, attackers are forced to string together multiple less severe vulnerabilities to get from point A to point B.



Microsoft Windows Vulnerabilities (2017-2022)



Windows critical vulnerabilities continue to trend downwards, following Windows 7 EOL and the shift to virtualization-based security (VBS).

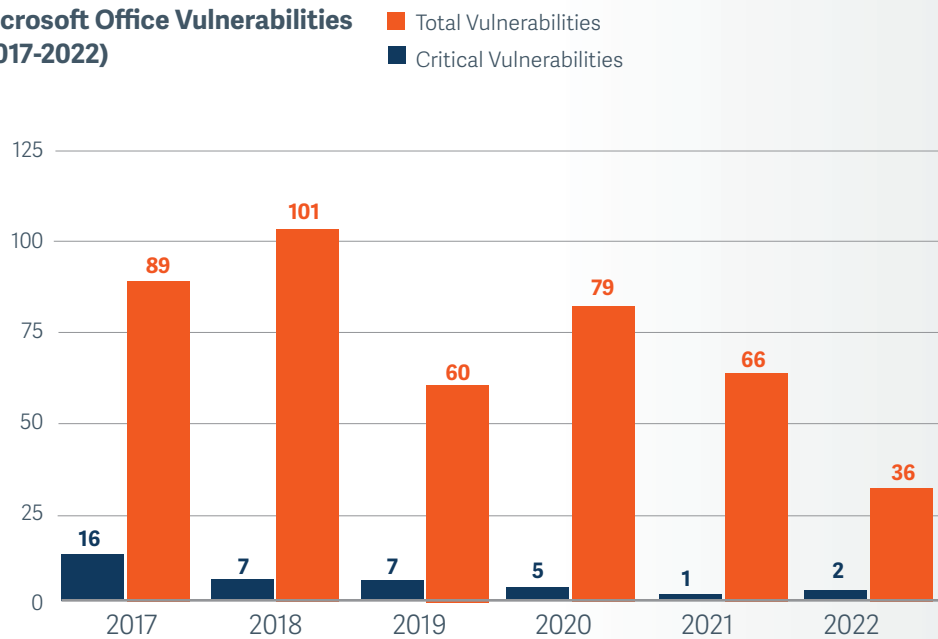
In 2020, the end of Windows 7 support forced users to upgrade to the Windows 10 operating system, eliminating many known vulnerabilities. This accounted for the steep, 44% drop in the number of Microsoft Windows vulnerabilities from 2020 to 2021.

Windows 10 has been around since 2015, and Windows 11, while only launched in 2021, shares the same core as Windows 10. This means the OS is less likely to introduce any major new vulnerabilities. Moreover, some security issues have been addressed by using virtualization-based security (VBS). VBS isolates untrusted websites and Office documents from the user data and protects key areas, such as credential stores, by providing hardware-level isolation and preventing pass-the-hash type attacks. This helps ensure protection even in the event the OS is compromised.

While Windows total vulnerabilities increased slightly in 2022 (returning to near 2018 levels), Windows critical vulnerabilities have continued a downward trend since these changes came into play. We expect an overall downward trend to continue, although progress will come in small increments because there remains a lot of legacy code.



Microsoft Office Vulnerabilities (2017-2022)



The Microsoft Office Suite has matured extensively over the past few years, driving down vulnerabilities and cutting off attack vectors, but the road to remediation has been a bumpy one in 2022.

The Microsoft Office products category experienced a 45% drop in vulnerabilities in 2022, while critical vulnerabilities increased from a low of one in 2021 to two instances in 2022.

While there is an overarching downward trend in the number of Microsoft Office vulnerabilities that stretches back five years, Office applications have remained a successful target for threat actors. This is largely due to the lag times between discovery and patching, as demonstrated by CVE-2022-30190 and CVE-2022-34713, both detailed below.

Along with patching vulnerabilities, Microsoft has been pushing to cut off common attack vectors, such as VBA macros in documents, that have been delivered from the internet. This is an extremely common attack vector, but previous mitigation attempts have merely been soft blocks that are easily circumvented by socially engineering the end user into enabling macros.

In 2022, Microsoft stepped up defenses against this attack vector by blocking internet macros by default in Office applications. The block did not go as smoothly as planned. [Microsoft announced the move in February, rolled it out in April, and temporarily rolled back the decision](#) before communicating another update about [blocking VBA macros by default in the summer](#)—after receiving user feedback. This caused considerable confusion.

So, while we have seen the trends around Microsoft Office vulnerabilities moving in the right direction, the road to remediation has been bumpy in 2022. Hopefully, moving forward, we will see a condensing of the lag times between discovery and patching.



Microsoft Office Vulnerabilities Spotlight

The Common Vulnerabilities and Exposures (CVE) system provides a reference method for publicly known information-security vulnerabilities and exposures.

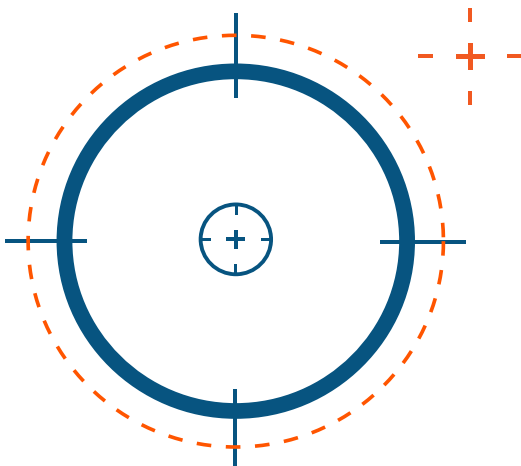
The Follina Exploit and CVE-2022-30190

CVSS base score of 7.8 and temporal score of 7.0

While you can never pick a favorite vulnerability, the “Follina” exploit that led to Office vulnerability CVE-2022-30190 certainly was memorable. This was a zero-day exploit that allowed for Remote Code Execution in Office products. Notably, it leveraged the Microsoft Office protocol and MSDT, a Microsoft support tool used to allow code to run, even if macros were disabled or when the user simply opened a preview of the file. Follina was quickly exploited by threat actors in various attack campaigns.

The timeline and response to this vulnerability was particularly interesting. As early as 2021, researchers [raised the issue of abusing Office protocols](#); however, it was initially dismissed as a non-issue. Over April and May of 2022, we began to see reports of these techniques being used in the wild. Other reports were submitted to Microsoft, yet no CVE appeared until May 30th. Finally, on the 14th of June, a patch was released. However, by this point, Qakbot and various other threat actors were actively exploiting the vulnerability.

**Read more about the
Follina exploit [here](#)**





DogWalk and CVE-2022-34713

CVSS base score of 7.8 and temporal score of 7.2

Related to Follina, [DogWalk \(CVE-2022-34713\)](#) also exploited the Microsoft support tool MSDT. DogWalk was first reported to Microsoft in late 2019, but Microsoft [initially took a dismissive stance](#) toward the potential impact and significance of the vulnerability. This was surprising, given that the vulnerability allowed an attacker to gain code execution by dropping an executable file into a Windows start-up folder when the victim opened a diagcab file.

Because browsers did not view diagcab files as a threat, it made it possible to perform a drive-by-download and trigger the exploit just by visiting a malicious website. In turn, it also provided a way to bypass the “Mark of the web,” where files are marked as coming from the internet and, therefore, treated with a lower degree of trust (something that many security solutions monitor). Finally, DogWalk provided a straightforward way to gain both execution and persistence by launching payloads on start-up.

Only after reports surfaced of the DogWalk zero-day being exploited in the wild, combined with fresh news of the Follina vulnerability, did Microsoft make a U-turn. In August of 2022, Microsoft decided this was a vulnerability to patch and [released a security update](#).

What can we learn from DogWalk and Follina? The importance of proactively recognizing and mitigating vulnerabilities.

While DogWalk was not strictly an Office vulnerability, it's worth highlighting alongside Follina because they both tell a story of the confusion that is caused when researchers disclose vulnerabilities, Microsoft initially dismisses the findings, and customers become caught in the middle.

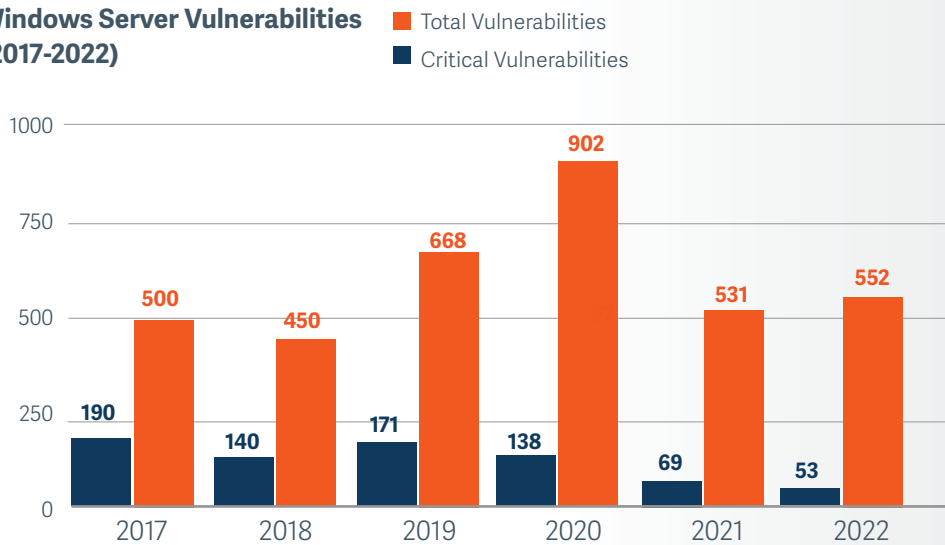
The lines between vulnerabilities, bugs, and ‘working as intended’ can become very blurred. Often, the discovery of these kinds of issues just scratches the surface of a much larger issue.

When Microsoft initially decides something isn't a vulnerability, it only causes security researchers and threat actors to start to pull at the threads to see what else can be unravelled. We'll talk about this more in a later section on the “vulnerability snowball effect.”

The main challenge here is getting impactful vulnerabilities recognized as such sooner and patched faster, rather than relying on in-the-wild exploits and social media pressure to drive the process.



Windows Server Vulnerabilities (2017-2022)



While Windows Server total and critical vulnerabilities are on a 4-year decline, patching coverage remains a concern.

The Windows Server category experienced a 4% increase in total vulnerabilities year-over-year, while the number of critical Windows Server vulnerabilities continued its multi-year decline, falling by a noteworthy 23% year-over-year. The number of Windows Server critical vulnerabilities has decreased by an impressive 72% since 2017.

One concern with regard to Windows Server vulnerabilities is the patching coverage. The [Shadowserver Foundation](#) reported that, in late December of 2022, nearly 70,000 Microsoft Exchange Server implementations were still vulnerable to the ProxyNotShell vulnerabilities (CVE-2022-41040 & CVE-2022-41082), which were discovered in September of 2022.

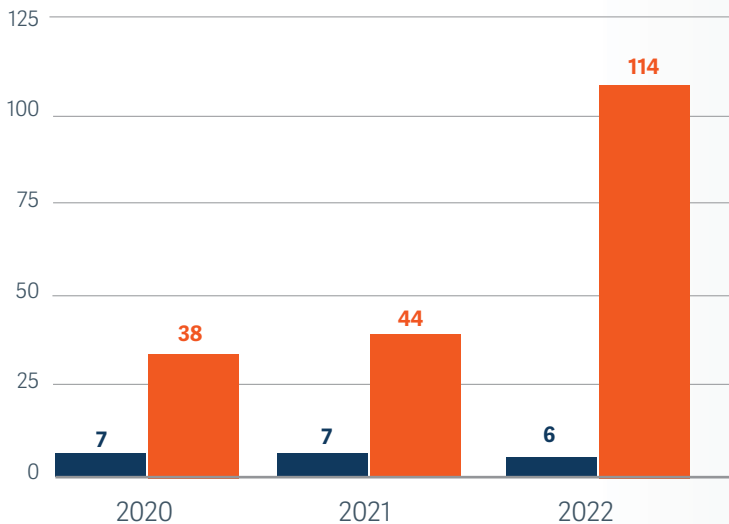
As with the Windows Print Spooler vulnerabilities (detailed below), even when patched, ProxyNotShell has continued to cause issues. In December of 2022, researchers from [CrowdStrike](#) discovered “OWASSRF,” a method for bypassing the mitigations Microsoft had provided. The OWASSRF exploit has been used by a number of ransomware threat actors, including during the attacks on H-Hotels and Rackspace.

This situation stoked some controversy. For instance, some organizations [reportedly held off patching](#) due to reports of authentication errors that could have caused downtime, and due to concerns that the patch could be bypassed anyway. These kinds of trade-offs between keeping servers up and running—and keeping them secure—can induce cold sweats in IT decision-makers.



Azure & Dynamics 365 Vulnerabilities (2020-2022)

■ Total Vulnerabilities
■ Critical Vulnerabilities



Microsoft Azure and Dynamics 365 experienced the largest increase in vulnerabilities of all Microsoft product categories in 2022, skyrocketing from 44 in 2021 to 114 last year, an increase of 159%.

Given the broad range of products Microsoft Azure and Dynamics 365 now covers, this increase might not be a huge surprise; however, one particular tool seems to have accounted for the majority of the vulnerability growth.

The Azure Site Recovery VMware to Azure tool alone was responsible for 80 vulnerabilities in 2022. Given this suite is part of a disaster recovery service that can automatically fail-over workloads to a secondary location when a problem is detected, it is equally concerning and reassuring to see so many vulnerabilities being remediated.

The majority of the Azure Site Recovery vulnerabilities were categorized as Elevation of Privilege and seem to share a root cause of SQL injection (SQLi). The fact that SQLi has been in the [OWASP Top 10 list](#), which charts the most common issues in web application security, serves as a timely reminder that we need to learn the lessons of the past.



The Vulnerability Snowball Effect

Each year, we seek to provide an answer to the question: **what do the trends mean?** Sometimes that answer lies as much in human nature as in any technical reason.

We know that the Microsoft ecosystem is vast and provides an ever-growing potential attack surface.

While most of the new code added is developed through secure development practices and is less likely to introduce new vulnerabilities than in earlier years, there is still a longtail of legacy code that much of the ecosystem is built on.

In the case of the Windows operating system, each version has been an evolution of the previous version—not a total rewrite. This means that, while the Windows NT kernel has evolved a long way since 1993, it has also brought along a lot of baggage.

This is where human nature enters. Every so often, researchers stumble across an area that proves to be a goldmine of vulnerabilities. One vulnerability is found and patched, but in the process, this draws fresh attention to an area that may have evaded scrutiny in the past. New researchers dig in, only to find new vulnerabilities, new attack vectors, and new ways around previous patches—and the vulnerability count starts to snowball.

The vulnerability snowball effect in action: The Print Spooler service

The Print Spooler service contains code that is over 20 years old and offers a clear example of how, even when patched, a vulnerability can continue to cause issues.

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.



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 straight-forward 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.

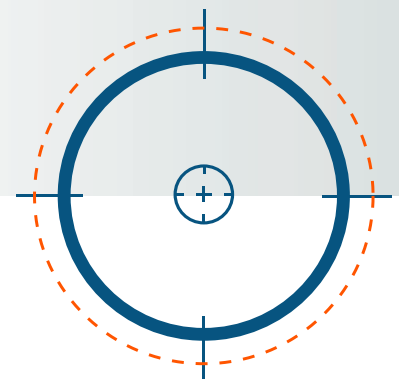
CVE-2022-44681, CVE-2022-44678, CVE-2022-41073, CVE-2022-38028, CVE-2022-38005, CVE-2022-35793, CVE-2022-30226, CVE-2022-30206, CVE-2022-30138, CVE-2022-29140, CVE-2022-29132, CVE-2022-29114, CVE-2022-29104, CVE-2022-26803, CVE-2022-26802, CVE-2022-26801, CVE-2022-26798, CVE-2022-26797, CVE-2022-26796, 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

What lessons can we learn from this?

As the saying goes, 'where there's smoke, there's fire.'

Keep an eye out for these emerging threats so you can make more informed decisions. For example, if you saw a rising trend in vulnerabilities associated with the Windows Print Spooler, while you may not have stopped a zero-day attack, you could at least have made sure you understood what your exposure was and what the potential mitigations were.

You might have disabled the Print Spooler service where it wasn't necessary, you might have made sure you knew which systems were exposed, and you might have dug into the settings and controls that could be applied to change the behavior. None of this prevents vulnerabilities, or prevents them from being discovered, but it makes your organization better poised to protect itself, as well as your customers and partners.





What does ChatGPT say?

One of hot technology topics of 2022, and so far in 2023, is ChatGPT, an AI chatbot. The next generation of AI chatbots has the potential to disrupt everything from your kids' homework to your IT incident response.

Microsoft has heavily invested in ChatGPT developer OpenAI since 2019, and has aggressive plans to integrate AI into a number of their products. ChatGPT is already being incorporated into the Microsoft search engine, Bing, with the hope of finally making it a stronger search competitor to Google—although we are not convinced we will all be saying “let me Bing that for you” or “have you tried Binging the answer” in 2023.

But what do these AI developments mean for the vulnerability landscape and reports?

Before delving into our cybersecurity expert commentary, we thought it would be a worthy and timely exercise to ask ChatGPT a couple questions.



What do you think about the Microsoft Vulnerabilities report by BeyondTrust?



As an AI language model, I do not have personal opinions. However, I can provide information and context about the Microsoft Vulnerabilities report by BeyondTrust that you mentioned.



The Microsoft Vulnerabilities report by BeyondTrust is an annual report that provides information about the state of security for Microsoft products and services. The report typically includes data on the number and types of vulnerabilities discovered in Microsoft products, as well as trends and insights into the state of security for Microsoft products.

Reports like this can be valuable for organizations that use Microsoft products and services, as they provide a snapshot of the current state of security and can help organizations prioritize their security efforts. However, it's important to keep in mind that the information in these reports is subject to change and should be considered in the context of a larger security strategy.

Additionally, it's important for organizations to stay informed about security threats and best practices for protecting their systems, regardless of the specific products and services they use. This can include regular security audits, software updates and patches, and ongoing education and training for employees.



When it comes to vulnerabilities, one of the general challenges with AI and ML is the transparency and explainability of the models used. This means that, not only could **AI introduce entirely new classes of vulnerabilities**, but the vulnerabilities might also be even **harder to track down and fix**.

AI vulnerabilities are usually different than traditional bugs in code, where one or more lines of code can be pointed to as the cause and fixed. AI learns from often vast data sets and fundamentally expands the entities that can be used to exploit a system.

If we consider that the misinformation spread online that is consumed by AI could be leading to dangerous responses and decisions, we start to see where issues could emerge. We can also think about physical objects, like a hand-drawn cardboard stop sign that causes your car to come to a halt when the in-car AI mistakes it for a real stop sign.



Will AI introduce a new class of security vulnerabilities?



Yes, it is possible that artificial intelligence (AI) will introduce new security vulnerabilities. As AI systems become more widespread and integrated into critical infrastructure, their potential for harm also increases. Additionally, AI systems can be vulnerable to manipulation and exploitation by malicious actors, who could use AI to carry out cyber attacks or gain unauthorized access to sensitive information.



For example, AI systems that rely on machine learning algorithms can be vulnerable to adversarial attacks, in which attackers manipulate input data to cause the AI system to behave in unexpected or harmful ways. AI systems that process sensitive information may also be vulnerable to data breaches, as attackers seek to steal valuable information or manipulate AI systems for their own gain.

It is important for organizations to be proactive in addressing the potential security risks posed by AI, by incorporating security measures into the design and implementation of AI systems and by staying informed about emerging threats and best practices for protecting AI systems.



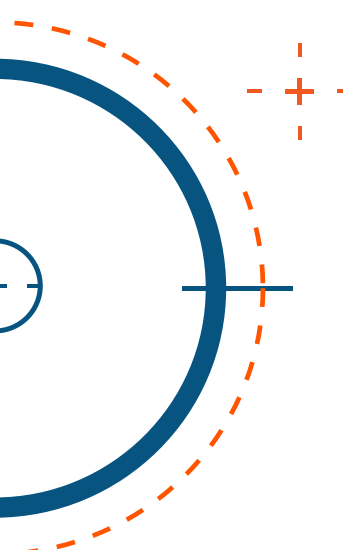
A 2022 paper titled [“Do Users Write More Insecure Code with AI Assistants?”](#) reported that researchers from Stanford found that developers using AI assistants to write code are more likely to introduce security vulnerabilities than those who don't rely on AI assistants.

At the same time, the users of AI assistants were more likely to believe they were writing more secure code than their non-AI augmented counterparts.

The Stanford researchers wrote, “We found that participants with access to an AI assistant often produced more security vulnerabilities than those without access, with particularly significant results for string encryption and SQL injection.”

While the Stanford study was limited in scope, it provides valuable insight into the hidden risks of AI—**its capacity to both introduce risk, while, at the same time, reducing our perception of risk.**

As Microsoft starts to harness more AI capabilities in their products, it will interest us greatly to see what impact this has on the volume and severity of their published vulnerabilities. Having made such significant strides forward in security since the famous [2002 Trustworthy Computing Memo from Bill Gates](#), we can only hope that [Bill's more recent words](#) comparing AI to nuclear energy—“both promising and dangerous”—don't go unheeded.





What Do the Experts Say?

Jane Frankland

CEO, KnewStart
Founder, IN Security Movement

Derek Hanson

Vice President Solutions
Architecture & Alliances, Yubico

Charles Henderson

Global Managing Partner,
Head of X-Force, IBM

Troy Hunt

Founder & CEO, Have I Been Pwned,
Microsoft Regional Director & MVP

Paula Januszkiewicz

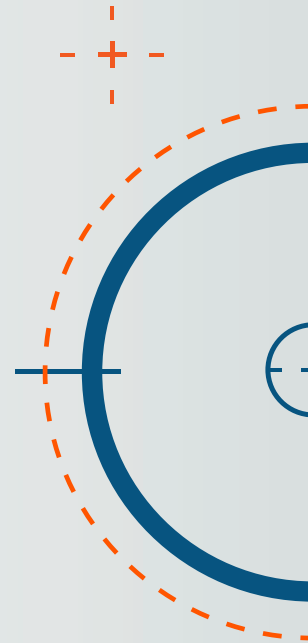
CEO, CQURE

Marc Maiffret

Chief Technology Officer, BeyondTrust

Avi Shua

CEO & Co-Founder, Orca Security



[LinkedIn](#) | [Twitter](#)

Jane Frankland

CEO, KnewStart

Founder, IN Security Movement



COMMENTARY

Cybersecurity is an ever-changing field, with new threats and technologies emerging every day and often making media headlines. Last year, we saw cybercriminals take advantage of remote working practices – which tie directly with the Covid 19 pandemic – to launch unprecedented attacks against business networks across the globe.

Furthermore, as deepfakes, AI-generated phishing emails, and other sophisticated methods of social engineering become cheaper and more commonplace, we're seeing more and more struggling to protect themselves from data breaches and compliance failures.

BeyondTrust's Microsoft Vulnerabilities Report highlights that Microsoft vulnerabilities are still rising year on year and that hackers are continuing to use identity theft as an attack vector - with the numbers of remote code execution and privilege elevation to reach their targets rising. However, it also reveals that the number of critical vulnerabilities within these attacks are decreasing.

As critical vulnerabilities have hit their lowest level in ten years, the report suggests that a successful attack now requires more advanced skillsets and tooling, thus potentially reducing the number of prospective attackers.

This is great news. Microsoft has put a lot of resources into security advancements over the years, and it's paying off.

Many of Microsoft's products have supported long-term versions, which allows organisations to transition safely to newer and more secure products and SaaS instances where everyone stays up to date.

Given the current threat landscape and the information contained within BeyondTrust's report, going into 2023, security leaders would be wise to enforce least privilege and monitor identity access to help them protect against future threats, including loss of revenue, IP, reputation, and fines. They can further stay ahead of the game by transitioning from less effective Multi Factor Authentication (MFA) methods, like SMS and mobile apps, to higher quality hardware authenticators, with FIDO authentication for added phishing-resistant protection.

These should be combined with other best practices, like embedding security into business priorities, building security awareness amongst staff and suppliers, keeping software up to date with the latest security patches, monitoring the network for suspicious activity, having an effective vulnerability management program in place, as well as ensuring they have an incident response plan that's well-rehearsed, and backing up data.



[LinkedIn](#) | [Twitter](#) | [Website](#)

Derek Hanson

Vice President

Solutions Architecture & Alliances

Yubico



COMMENTARY

Just as cyberattacks have increased on a global scale, Microsoft has seen a striking rise in vulnerabilities. The 10-year trend analysis in this report offers unique and valuable insights for security professionals looking to secure their organization against current and future threats. Let's first take a look at the current threats.

Gaining admin access to user systems has always been like striking a gold mine for attackers. The damage from gaining access to a single privileged account is catastrophic for many organizations, and responsible for a growing number of data breaches in the headlines. As this report shows, it's critical for organizations to implement least privilege and remove unnecessary admin rights to proactively mitigate vulnerabilities.

And what do future threats look like? Well as William Gibson once said, "the future is here—it's just not widely distributed". We are witness to the evolution of machine learning and artificial intelligence—happening right now, in front of our eyes. These technologies are beginning to be applied to create dystopian-esque "deep fakes" of both voices and faces. They can create synthetic replicas of the same characteristics that many biometric solutions can validate during authentication.

As deep fake technology becomes more accessible and easier to produce in the physical world, the impact on the industry's authentication solutions that leverage

biometrics will increase. Solutions that leverage remote biometrics for identity matching will either evolve to detect this technology or be left behind. Today, and going forward for advanced protection, biometric solutions need to be backed by modern, hardware-based authenticators, such as security keys, that work across platforms and add an additional layer of security to these options.

To summarize, it is imperative that organizations address current threats by implementing strategies such as least privilege and monitoring identity access to reduce the risk (should the worst happen). It is also critical for security professionals to stay ahead of the curve and consider moving away from legacy multi-factor authentication (MFA) methods, such as SMS and mobile apps – and towards portable, hardware authenticators based on modern FIDO authentication that offer phishing-resistant MFA capabilities.

We may be in a world where the lines between science fiction and reality are starting to blur, but in this fast-moving arms race, we already have highly effective, phishing-resistant authentication solutions—and privileged access management solutions—that give us the provable and trusted security we need.

[LinkedIn](#) | [Twitter](#)

Charles Henderson

Global Managing Partner, Head of X-Force IBM



COMMENTARY

In today's cyber threat landscape, businesses face an impossible task of chasing down every single vulnerability due to the sheer volume disclosed every year. While exploits can still lead to major incidents, not every vulnerability and exploit require the same attention. Attackers tend to focus on the vulnerabilities and exploits that work for their operations, and onboarding a new exploit or vulnerability requires a new attack path and additional investments.

This Microsoft Vulnerabilities Report from BeyondTrust showcases the concerning rise in vulnerabilities. Add to this the time and resources required to patch or find a workaround and it's no wonder businesses are finding it increasingly challenging to keep up with vulnerable management practices. Focusing on patching alone is no longer feasible; cybercriminals have access to thousands of exploits, and the cyber community continues to battle a shortfall of talent and financial resources that are being stretched to their limits.

Businesses must prioritize threat-driven vulnerability management programs and implementation of least privilege to reduce risk. By understanding how attackers operate and leverage vulnerability exploitation to accomplish their objectives, businesses can prioritize their vulnerability management efforts based on the risk and potential impact to their business. This also results in a much more manageable list of vulnerabilities.

The same threat-driven approach can be extended into how organizations think about zero-day exploits. While zero-day exploitation is given a lot of attention within the media, observing vulnerability trends shows that zero-

day discovery is dwarfed by the number of existing vulnerabilities, and organizations are unable to keep up with patching.

Analyzing X-Force's culminative vulnerability and exploit database shows that, while vulnerability discovery has rapidly increased year-over-year, only 3% of vulnerabilities were associated with a zero day. Furthermore, analyzing attacker behaviors indicates that attackers favor exploitation of older known vulnerabilities rather than discovering or leveraging the latest and greatest zero-day exploits.

In 2022, WannaCry (leveraging a vulnerability from 2017) was the second most frequent ransomware variant observed by X-Force. Threat-driven vulnerability management allows organizations to exit the vicious vulnerability and zero-day fire drill cycle and really move the needle in terms of risk reduction by focusing patch efforts on the vulnerabilities that are most likely to be adopted by attackers and to cause the biggest impact on the organization's mission. For the sea of vulnerabilities and exploits left over, businesses should allocate resources to detect and respond to the behaviors that indicate exploitation, regardless of the vulnerability used.

By improving detection and response capabilities, businesses can make it more difficult for attackers to complete their goals, even if they are able to gain access through vulnerability exploitation.



[LinkedIn](#) | [Twitter](#) | [Website](#)

Troy Hunt

Founder & CEO, Have I Been Pwned, Microsoft Regional Director & MVP



COMMENTARY

I was invited to the Association of Superannuation Funds of Australia Annual Conference recently (that's our version of compulsory retirement savings) where I talked to an audience of finance people about the world of cybersecurity.

Only 6 months earlier, it's unlikely I would have been invited at all, but two massive data breaches Down Under (one a major telco, the other our largest private health insurer), each exposing data for almost half our population, had piqued the interest of the masses—and corporate boards.

So, in front of an audience of money industry executives, I spoke about a topic unfamiliar to most, but one that everyone had front-of-mind. You couldn't not have cybersecurity front-of-mind because it had dominated our news headlines for months, and that in itself is noteworthy. Cybersecurity is now a mainstream topic that everyone is aware of because we've either been impacted by it directly (I myself am in dozens of data breaches... that I know of), exposed to it non-stop in the media, or because it's become a common backyard barbeque topic.

Inevitably, the AI question came up at the event – **“will AI help?”** – to which the answer is obvious: **yes.**

Less obvious, is who it helps. Whilst it was a little hard to see the precise reactions of the audience from behind the stage lighting, it was clear that the benefit to the bad guys isn't something that had previously dawned on most people.

Which brings us to the moral neutrality of technology. Just as encryption is beneficial to securely making a payment online whilst simultaneously being beneficial to organised crime, so too does AI benefit both sides.

I mean, how much better is ChatGPT at writing a legitimate sounding phishing email than your average scammer? Exactly!

All of this makes for a fascinating infosec landscape, with each side rapidly getting better at their respective objectives, whilst an unprecedented number of people watch on from the sidelines, often becoming unwilling participants in the digital crimes.



Paula Januszkiewicz

CEO
CQURE



COMMENTARY

Over the past year, I have observed cyber events affecting millions of people across the globe. Nowadays, corporate infrastructures are exposed to new external attack vectors and threats. However, apart from dangers arising from working remotely, the 2020s are the decade of faster attacks containing rapidly evolving deepfakes, sophisticated, AI-generated phishing emails, and other more advanced social engineering actions. We can expect that, in 2023, the number of cyber threats will continue to evolve and increase.

Thanks to the Microsoft Vulnerabilities Report, published by BeyondTrust, we are able to conclude that hackers' objectives remain unchanged, keeping an emphasis on remote code execution and elevation of privileges. Every attack happens by using some identity that has higher or lower privileges, and every attack involves the execution of malicious software, whether it is a script or an executable, and whether we are dealing with process injection, or just simple means used by hackers to perform phishing.

Malicious attack vectors, including AI/Deepfakes, used in communication with a target, have changed. Yet, regardless of the point of entry—even the simplest one—a successful cyberattack may result in an extensive financial loss and disclosure of confidential information.

This is why it is strongly recommended to perform regular cybersecurity strategy reviews and various types of penetration tests, as they are one of the most efficient ways to identify technical vulnerabilities in the company's IT infrastructure before an attack occurs. I think that audits and constant efforts to improve security are features that characterize organizations with mature cybersecurity policies.

However, I find it promising that Microsoft's critical vulnerabilities hit their lowest number in the ten-year history of the Microsoft Vulnerabilities Report. Theoretically, it means that a successful attack requires a higher level of the hacker's skillset and tooling, so the number of possible adversaries should be reduced.

Considering this latest edition of the Microsoft Vulnerabilities Report, I am expecting 2023 to be a year of incident response readiness debate. All organizations should revise their own security goals and prepare well-written and well-tested incident response plans. Other critical aspects include monitoring, as well as privileged access and identity management. When the attack happens, the first thing an attacker needs is identity. Therefore, it is impossible to build a secure ecosystem without rethinking our corporate approach again and again.



[LinkedIn](#) | [Twitter](#) | [Website](#)

Marc Maiffret

Chief Technology Officer BeyondTrust



COMMENTARY

As CTO of BeyondTrust, and someone with a long history of calling attention to Microsoft vulnerabilities, it is rewarding to see this report celebrating a 10-year anniversary and continuing to highlight the need to keep improving security at Microsoft.

In the early 2000s, I created security research teams with the goal of galvanizing Microsoft and other companies to make security a serious focus. Since those days, Microsoft has made substantive strides forward to improve the security of their code and systems. Clearly, vulnerabilities remain, and as we can see in this year's report, they are hitting a record high—but we can also see where their investment in security has paid off, with fewer critical vulnerabilities than ever before.

Looking back at the changes over the past decade, we can see that security is no longer viewed as a third-party bolt-on to the operating system, but as something that should be baked in. There are lots of technical examples of this in the latest generations of the Windows OS, which are far more hardened and secure by default. These architectural changes are a big factor in reducing the number of critical vulnerabilities.

But we shouldn't relax too much.

There are still plenty of vulnerabilities to discover. The collection of print spooler service vulnerabilities discovered over 2022 have shown us Microsoft's "Print Nightmare" that started in 2021 is not over yet. Beyond that, there remain many undiscovered vulnerabilities—some decades old—lurking within Microsoft environments for researchers and threat actors to explore.

One thing this report has highlighted so well over the years is how both patching and the timeless concept of least privilege are essential to mitigate the risks organizations face. With Remote Code Execution (RCE) remaining one of the top vulnerability categories over the past decade, we need to ensure we are applying least privilege across all our estates, on-prem, hybrid, and cloud to ensure any RCE exploits don't provide an attacker with excessive privileges. It is critical to create the hurdles an attacker can trip over when attempting to exploit a zero day or known vulnerability.

Stay safe!

Marc



LinkedIn | Website

Avi Shua

CEO & Co-Founder

Orca Security



COMMENTARY

Vulnerabilities are still the largest attack vector in the cloud, and the findings of this year's Microsoft Vulnerabilities Report reaffirm this with resounding effect. With a huge, 159% YoY increase in Azure and Dynamics 365 vulnerabilities, companies need to be more vigilant than ever when it comes to patching and security strategies. A big part of mitigating risk begins with least privilege – this has been a significant step for many years (and still is) when it comes to cloud systems and IoT devices.

Perhaps now more than ever, organizations are understanding the critical need to prioritize issues based on the potential blast radius and business impact of a risk. This can only be accomplished when organizations have wide visibility and contextual insight into their environments. As this report demonstrates, critical vulnerabilities carry contextual threat levels and impact, especially considering Microsoft's unique severity rating system.

I'll illustrate this with the following example: Server 1 and Server 2 are both web servers that are using a vulnerable library (CVE-2018-1176). Without context, the risks on Server 1 and Server 2 seem to be the same. However, with access to contextual data, we see that Server 1 is Internet-facing and easily accessible to attackers.

In addition, Server 1 exposes a key to an adjacent asset that contains PII. Therefore, the CVE on Server 1 should be scored as high risk. On the other hand, Server 2 is an intranet server that is not publicly accessible and exposes no other exploitable risks. Therefore, this CVE poses a minimal threat and should be scored as informational only.

In last year's [Public Cloud Security Report](#), 78% of identified attack paths use known vulnerabilities (CVEs) as an initial access attack vector and, on average, require only three steps to reach "crown jewel" data. The good news is that most attacker entry points can be prevented relatively easily since these CVEs are known, most have remediations available, and usually, only a very small percentage of them are externally exposed. When admin rights are removed and identities are effectively secured, the decrease in risk is even more significant.

With contextual insight and effective risk prioritization, cloud security teams can remediate strategically, fix the most dangerous risks first, and work smarter, not harder. In addition, by taking preventive measures to reduce an attacker's ability to move laterally, such as controlling privileged access, organizations can ensure that, even if an attacker does gain access, the potential damage is minimized and restricted.



Mitigating Microsoft-Based Vulnerability Risks

Timely patching is an important way to minimize the chance of a vulnerability-related breach.

Yet, with this strategy alone, organizations will still be at risk of zero-day exploits. In addition, patching vulnerabilities is not always practical or desired by an organization. That's why it's crucial to have proactive security defenses, such as a least privilege posture, in place.

5 Indispensable Mitigation Strategies for Securing Your Microsoft Environment:

- 1 Implement vulnerability management:** Find, prioritize, and determine a remediation path for all vulnerabilities. Keep in mind that patching sooner than later can also help you prevent a seemingly innocuous vulnerability from snowballing into a bigger threat.
- 2 Enforce least privilege, such as by removing local admin rights:** 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 where the data was available. That means that, without admin rights, the vulnerability cannot be exploited—even if it remains unpatched. A least privilege approach, which is also a core part 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.
- 3 Follow security hardening protocols:** 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.
- 4 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, in particular, 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.
- 5 Stay vigilant regarding emerging threats:** Understanding the threats goes a long way toward making more informed decisions and keeping yourself secure. The past decade has ushered in considerable changes in the Microsoft threat landscape, and 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.



When it comes to reducing the risk associated with Microsoft critical vulnerabilities, BeyondTrust Privileged Access Management (PAM) delivers a robust range of benefits.

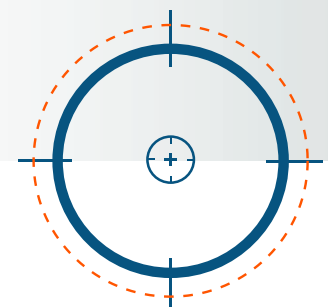
BeyondTrust protects privileged identities, right-sizes privileges, and secures and audits privileged access across the enterprise.

Customers leverage BeyondTrust Privileged Access Management 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 and secrets that touch the enterprise.
- Manage, monitor, and audit every privileged session.
- Gain advanced visibility into potential attack pathways so access can be proactively right-sized and attack vectors eliminated.
- Satisfy rigorous compliance and forensic requirements by providing easy-to-access reporting on all privileged activity and other insights.
- Qualify for cyber insurance by meeting a number of key security controls demanded by cyber insurance providers and underwriters.

With BeyondTrust, organizations gain proactive protection against external threats (ransomware, malware, etc.) and insider threats.

[Learn more.](#)





What have we learned after a decade of Microsoft vulnerability analysis?

Conclusion

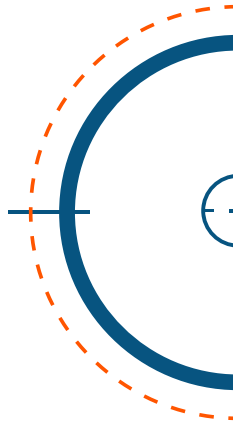
In 2022, the total number of Microsoft vulnerabilities hit a record-high, almost quadrupling since this report began a decade ago. Microsoft Elevation of Privilege vulnerabilities have soared 650% across the past ten years. Over that time, new Microsoft products have driven the overall increase in total vulnerabilities, with Azure and Dynamics 365 vulnerabilities climbing by 159% this last year alone.

While total Microsoft vulnerabilities continue to spike—symptomatic of a growing enterprise and its expanding attack surface—Microsoft’s threat reduction initiatives and dedication to the adoption of security patches and protocols has led to a steady, 5-year decline of critical vulnerabilities. In 2022, only 6.9% of Microsoft vulnerabilities were rated as ‘critical’, compared to 44% in 2013.

Roughly a decade ago (2014), Microsoft embarked on a mobile-first, cloud-first strategy. At the time, this strategy represented a shift, but today, these are foundations of Microsoft, and, increasingly, enterprises around the world. In the decade ahead, technologies once considered speculative, such as AI, will actively be honed, productized, and embedded across Microsoft and everywhere. While there is much promise in these technologies to help both organizations and humanity, they represent new attack surfaces and potential threat vectors. Vulnerabilities may emerge in ways that have never been seen before.

We have learned that, just like death and taxes, vulnerabilities (at least where software is concerned) are inevitable.

As the technology landscape continues its next phase of evolution, vulnerability numbers should continue to climb, new threats will continue to crawl out from the cyber-ether, and we’ll continue to offer our insights and defense tactics.





If there's one beacon of light shining across the past ten years of vulnerabilities, it's the fact that the fundamental ways to mitigate those risks have remained constant for well over a decade.

The concepts of least privilege outlined by the [US Department of Defense in 1985](#) are timeless. Least privilege enforcement has proved just as relevant to the cloud systems and IoT devices of today, as it did to the legacy systems (some of which are still operational) of yester-year.

Those organizations who successfully implement proactive and preventative security controls will continue to be much better poised to withstand tomorrow's threats, as they have been in the past decade. If there is one piece of advice you can take away from this report to help you secure your organization against unrelenting cyberthreats, it's to keep implementing and enforcing the foundational security controls that have proven themselves time and again against the decade's greatest threats.

Methodology

Every Tuesday, Microsoft issues "Patch Tuesday" and releases security bulletins announcing fixes for any vulnerabilities affecting Microsoft products. The BeyondTrust Microsoft Vulnerabilities Report, produced annually, 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 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, however, Microsoft shifted methodologies and moved to the Common Vulnerability Scoring System (CVSS). In 2022, 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.

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 applying 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

FREE TOOL [Privileged Access Discovery Application](#)

Utilize the most powerful free tool available to scan your environment and pinpoint overprivileged accounts, service accounts, unused accounts, privileged credentials, remote access tools, and more.

TAKE THE TEST 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.

WHITEPAPER [Cybersecurity Survival Guide](#)

Access the tips and strategies that can help you steer clear of the landmines in the cybersecurity landscape.

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.



BeyondTrust is the worldwide leader in intelligent identity and access security, empowering organizations to protect identities, stop threats, and deliver dynamic access to empower and secure a work-from-anywhere world. Our integrated products and platform offer the industry's most advanced privileged access management (PAM) solution, enabling organizations to quickly shrink their attack surface across traditional, cloud, and hybrid environments.

BeyondTrust protects all privileged identities, access, and endpoints across your IT environment from security threats, while creating a superior user experience and operational efficiencies. With a heritage of innovation and a staunch commitment to customers, BeyondTrust solutions are easy to deploy, manage, and scale as businesses evolve. We are trusted by 20,000 customers, including 75 of the Fortune 100, and a global partner network. Learn more at www.beyondtrust.com.

beyondtrust.com