BeyondTrust

2022 Microsoft Vulnerabilities Report

Despite Uneven Progress, a Picture of Elevated Vulnerabilities Remains

BeyondTrust

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Now in its ninth year, the Microsoft Vulnerabilities Report provides a unique analysis of the vulnerability landscape in Microsoft's ecosystem.

Historically, the report has delivered a holistic annual view of the vulnerabilities within Microsoft's platforms and products, and has established an undeniable business case for the importance of removing admin rights to reduce risk.

In November 2020, Microsoft announced they would be changing how they report their vulnerabilities in the Microsoft Security Update Guide.

This change involved switching over to the industry-standard **Common Vulnerability Scoring System (CVSS)**. While the new reporting system brings benefits – such as creating parity and opportunity for comparability with third-party bug reporting – it also creates some visibility challenges, which we will explore.

As with prior versions, this year's report findings will help you to better understand and address risks within the Microsoft ecosystem.

Highlights & Key Findings

After a steep 5-year rise, the total number of reported Microsoft vulnerabilities **dropped by 5% in 2021.**

But it's not merely the number of vulnerabilities that matters—**it's their potential impact.**

Does the vulnerability class of 2021 pose more danger and have a broader impact than its predecessors?

1. For the second year running, **Elevation of Privilege was the #1 vulnerability category** for the world's largest software company and 2nd largest cloud services provider.

2. Dissecting Microsoft's shift to CVSS reporting, it is now impossible to determine exactly how many vulnerabilities could be mitigated by removing admin rights. **Spoiler: the problem of excess privilege hasn't gone away.**

Along with the usual data breakdown, we will examine how these vulnerability trends, along with cloud security adoption, collectively influence how we should think about cybersecurity and risk management in 2022 and beyond. Additionally, this report will spotlight some of the most significant CVEs of 2021 (9.0+ CVSS severity scores), break down how they are leveraged by attackers, and articulate how you can prevent or mitigate them.

As always, a panel of some of the world's leading cybersecurity experts will weigh in on the report findings and share their perspective on how to manage risk in this ever-evolving threat environment.

> This is an edition like no other and makes for essential reading for security professionals around the world.

Data Highlights

Elevation of Privilege remains the **#1 vulnerability** category for the second year running, accounting for 49% of all vulnerabilities in 2021.

FROM 2015 TO 2020

removing admin rights **could have mitigated, on average, 75% of Critical vulnerabilities.**

In absence of this data for 2021 (due to the Microsoft reporting change), it is crucial that organizations do not overlook the pivotal risk-reduction step of removing admin rights.

47% DECREASE In Critical vulnerabilities YoY – *the lowest annual number since this report began*

349 Vulnerabilities in IE & Edge – *a record high*

40% DECREASE Windows vulnerabilities dropped YoY

50% DECREASE Critical vulnerabilities in Windows Server halved YoY

Microsoft Moves to Industry-Standard CVSS Format

Dating back to the 2002 Trustworthy Computing email Bill Gates sent to every full-time Microsoft employee, Microsoft has prioritized improving security and privacy.

Indeed, in the years to follow the launch of Trustworthy Computing (TWC), Microsoft has strived to bake security and privacy considerations and controls across their product and services portfolio.

Truth be told, they did need some nudges along the way *(we're looking at you, Windows 10)*. Since the inception of Patch Tuesday reporting all the way back in October 2003, Microsoft has provided software patches that feature key security updates.

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.

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.

Among other variations, Microsoft would include the following verbiage in the summary:

- *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*

With Microsoft's move to the Common Vulnerability Scoring System (CVSS), their vulnerabilities can now be cross-referenced more easily with third-party bugs.

This is a valuable benefit because it simplifies some analysis.

On the other hand, an unfortunate trade-off from this change is the loss of the ability to determine the impact of admin rights on Critical vulnerabilities.

Yet, 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 due solely to the reporting change, it's imperative that organizations don't get complacent and overlook the removal of admin rights as the must-do step that it is. Admin right removal also remains a key piece of applying a least privilege strategy, as well as for enabling zero trust.

What is CVSS?

COMMON VULNERABILITY SCORING SYSTEM

The Common Vulnerability Scoring System (CVSS) provides a way to capture the principal characteristics of a vulnerability and produces a numerical score reflecting a vulnerability's severity level, from 0 to 10.

While this is an industry-standard rating system, it does not allow security researchers or customers to precisely determine which vulnerabilities could have been mitigated by removing admin rights from end users.

It's important to consider that, when scoring vulnerabilities, you should not rely exclusively on the vendors' CVSS Base Score to prioritize risk and remediation plans.

End users should apply custom environment metrics to translate the risk to their own organizations. Guidance for this calculation can be found on the NIST website.

LOW	MEDIUM	HIGH	CRITICAL
0.1 - 3.9	4.0 - 6.9	7.0 - 8.9	9.0 - 10.0

Report Retrospective:
A Six-Year Summary

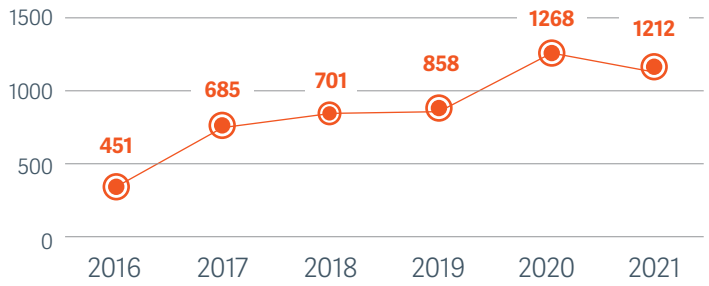
Before we parse through our Microsoft vulnerability findings and analysis across 2021, it's helpful to reflect on how Microsoft vulnerabilities have trended in recent years.

2016 - 2020

From 2016 to 2020, we saw Microsoft vulnerabilities more than double.

However, in 2021, for the first time since this report began, Microsoft vulnerabilities decreased (by 5%) – from a record high of 1,268 across 2020 - to 1,212 in 2021.

Total Number of Microsoft Vuinerabilities (2016 - 2021)



2019 - 2020

From 2019 to 2020, we witnessed the single greatest year-over-year rise in Microsoft vulnerabilities (48% YoY) to date.

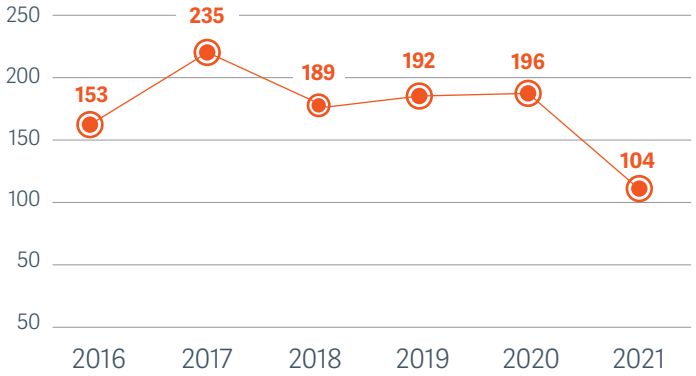
Coinciding with the time of this surge, attackers enjoyed heightened levels of opportunities due to the nascent coronavirus pandemic. The rapid shift to remote work, and hasty acceleration of digital transformation initiatives, left unprecedented volumes and variations of security holes for threat actors to find and target.

2020 - 2021

While the vulnerability wave crested in 2020, it pulled back slightly in 2021.

The most striking difference we observed between 2020 to 2021 was the year-over-year reduction in Critical vulnerabilities, which plummeted from 196 in 2020 to 104 in 2021. This represented a 47% decrease in Critical vulnerabilities from 2020 and marks an all-time low for this report.

Microsoft Critical Vuinerabilities (2016 - 2021)



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), Security Feature Bypass, Tampering, Information Disclosure, Denial of Service (DDoS), and Spoofing.

Since the first edition of this report in 2013, all the way through to 2019, Remote Code Execution always accounted for the highest proportion of vulnerabilities.

However in 2020, this trend abruptly ceased as the number of vulnerabilities in the Elevation of Privilege category skyrocketed and far surpassed other categories. In 2021, Elevation of Privilege vulnerabilities again towered above the other vulnerability categories.

Microsoft Vulnerability Categories (2016 - 2021)

	2021	2020	2019	2018	2017	2016
Remote Code Execution	326	345	323	292	301	269
Elevation of Privilege	588	559	198	145	90	114
Information Disclosure	129	179	177	153	193	102
Denial of Service	55	46	52	29	43	0
Spoofing	66	104	63	20	16	12
Tampering	3	7	8	8	1	0
Security Feature Bypass	44	30	38	20	41	26

Elevation of Privilege Vulnerabilities Take the Lead

We suspect the vertiginous rise in Elevation of Privilege vulnerabilities may reflect at least two key developments:

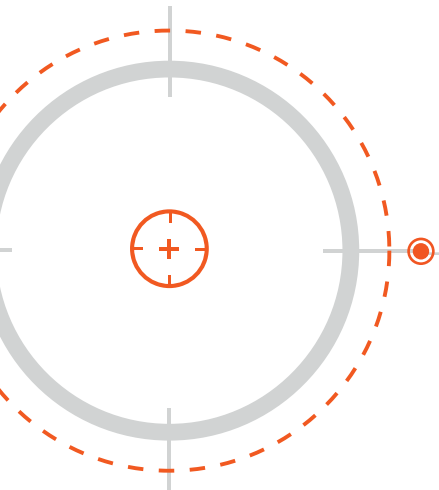
1. As organizations better adhere to security best practices and remove admin rights from users, attackers seek new ways to gain privileges. Without easy access to users with local admin rights, attackers have started to innovate to gain elevated privileges that can then be used to compromise systems, steal credentials, and move laterally.
2. The ever-increasing attack surface of cloud applications and systems provides an environment where elevated privileges are highly desirable to a threat actor. The security implementations to manage these dynamic—and sometimes ephemeral—privileges across cloud, hybrid, and multicloud environments are also typically less mature at organizations.

Many Vulnerability Categories Saw Drops, But This May Only Mask Over The Cracks

The number of vulnerabilities across some other categories, such as memory corruption, overflow, and cross-site scripting (XSS), plummeted across Microsoft products from 2020 to 2021, with 215 less collectively reported year-over-year.

For most IT environments, this represents welcome news. With that said, the reasons for these vulnerability reductions are slightly elusive. Was the drop due to A. better security and coding practices, B. the end of life for products like Windows 7, or C. the shift of services to the cloud? We believe it's a combination of all three.

Older, less secure software (such as XP and Windows 7) is not subjected to the same security diligence as newer products and services, so training and testing on these older platforms is no longer being maintained. Microsoft has also done a better job of creating solutions with less flaws, as well as proactively identifying and fixing vulnerabilities in cloud services without the explicit need to report them. Each of these efforts can go a long way toward reducing the number of reported vulnerabilities.



Key Takeaways

- Always ensure you are not using end-of-life software in your environment
- The cloud can provide a more efficient way of mitigating risks by removing the burden of remediation from your information security team

Remote Code Execution Vulnerabilities – *Mixed Results*

The number of Remote Code Execution vulnerabilities dropped slightly in 2021, back roughly to the level seen in 2019.

Of the 326 remote code execution vulnerabilities reported in 2021, 35 had a CVSS score of 9.0 or higher, according to CVEDetails.com.

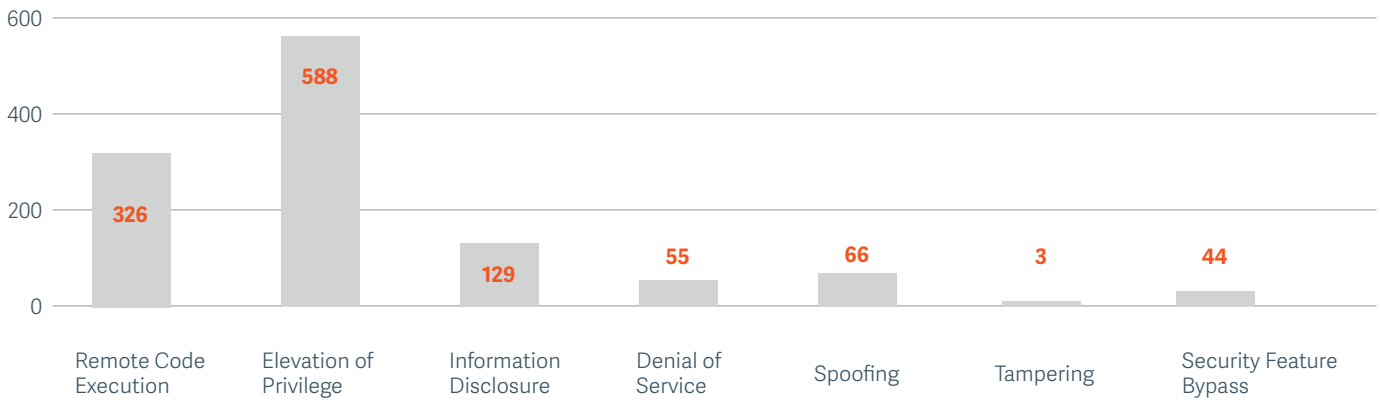
While some of these are vulnerabilities in the user space, and others affect applications and the operating system directly, all of them can be exploited without any user intervention.

If you consider the concept of least privilege for users and applications (including service accounts), an attacker exploiting these vulnerabilities will at least be able to operate with the privileges assigned to the user or application.

Without the extra information provided by the executive summaries in previous years, it is purely speculative—and requires penetration testing—to determine whether privilege escalation is even possible.

With this type of risk, a workable exploit is not a matter of "does an exploit exist", but rather "when will it be publicly available." It is a forgone conclusion that almost all vulnerabilities with a CVSS score of 10.0 (9 of 308) will make their way into commercial penetration testing tools and scripts used for pen testing assessments. Operating in an environment using least privilege is the best preventative defense for this type of risk.

Breakdown of Microsoft Vulnerability Categories (2021)



Vulnerabilities by Product

Internet Explorer & Edge
Windows
Microsoft Office
Windows Server
Azure & Dynamics 365

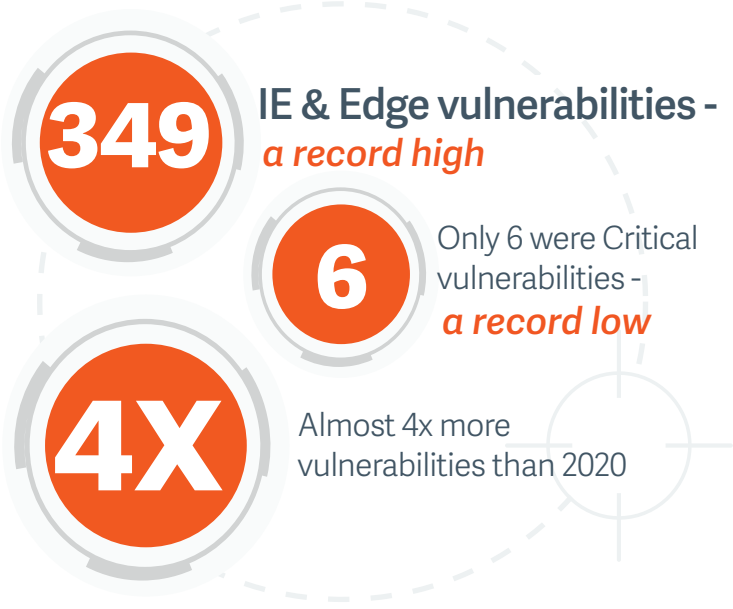
Internet Explorer & Edge Vulnerabilities

In January 2020, the Microsoft Edge browser moved to a Chromium-based engine, meaning that both Google Chrome and Edge could have the same flaws at the same time.

This increase in the base rendering code leaves no "safe" mainstream browser to use as a mitigation strategy to Edge vulnerabilities.

Since Microsoft Edge is based on Google's Chromium technology, vulnerabilities identified in Google's Chrome Internet Browser could also be in Microsoft Edge and need remediation.

In 2021, Google Chrome itself had 308 vulnerabilities, according to CVEDetails.com. The saving grace is that only 4 of the Google Chrome vulnerabilities were considered Critical. That said, the vulnerability total does support that Microsoft is inheriting flaws from Google.



Internet Explorer versions 9 and 11

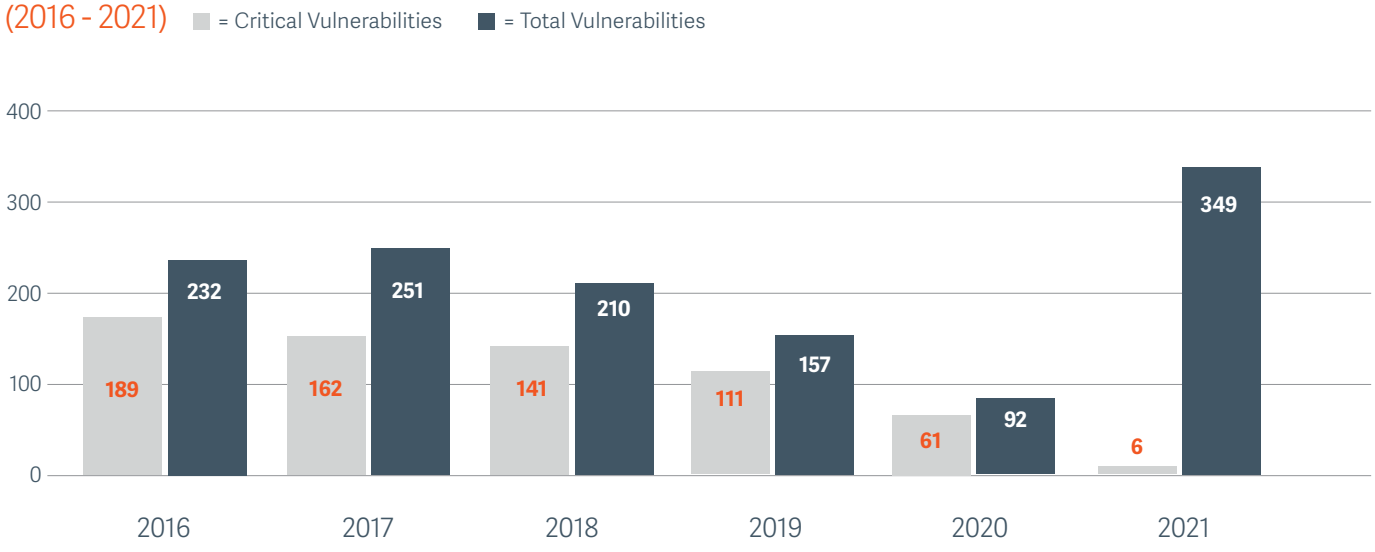
We believe **three key factors** are primarily responsible for spurring the sudden increase in Edge vulnerabilities.

1. **Consolidation of the browser market, as Edge moves to a shared Chromium base.** As legacy Internet Explorer browsers are phased out, threat actors are forced to focus on Edge and Chrome. This trend is further accelerated by the deprecation of commonly exploited plugins, such as Adobe Flash. Deprecation of these targeted plugins redirects focus on the browsers themselves.

2. **Google has increased transparency around vulnerability reporting and now offers more attractive financial incentives to report vulnerabilities.** In 2021, Google paid out around $3.1 million in bug bounty rewards for Chrome vulnerability reports.

3. **The number of Critical Microsoft vulnerabilities has diminished in areas where total vulnerabilities have significantly risen.** This dynamic likely reflects the security architecture improvements made to the browser. These improvements mean that attackers need to chain multiple exploits together to escape the browser and run code on the underlying system. Contrast this to previously, when an attacker might have relied on a single exploit to compromise a system. Now, threat actors are forced to find multiple non-critical vulnerabilities in the hope they can effectively chain them together in an attack.

Internet Explorer & Edge Vulnerabilities (2016 - 2021)



Windows Vulnerabilities

In 2020, we witnessed a record-breaking 907 vulnerabilities in aggregate across Windows 7, Windows RT, Windows 8/8.1, and Windows 10 operating systems.

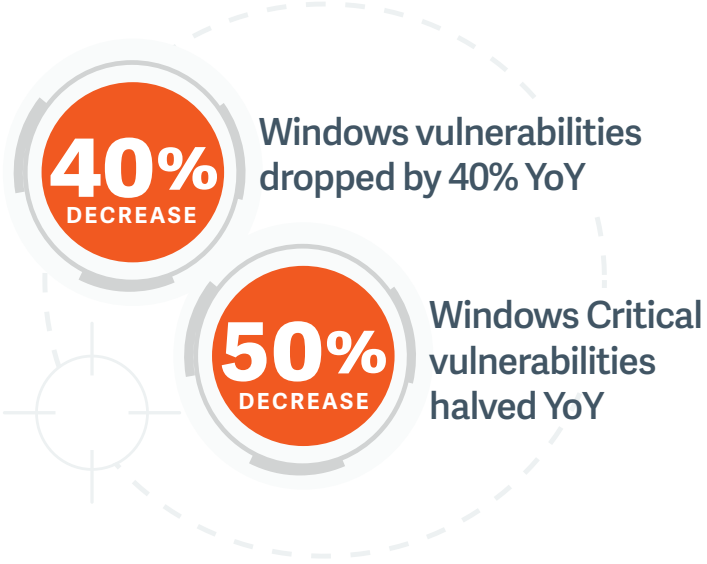
However, in 2021, the number of vulnerabilities across Windows OSs dropped to 507.

Windows 10 was touted as the most secure Windows OS to date when it was released. Yet, the Windows 10 OS still experienced 60 Critical vulnerabilities last year. With that said, the number of Critical Windows vulnerabilities has continued a downward trend. The number of total Windows vulnerabilities has now dipped slightly below pre-pandemic levels.

As Microsoft continues to bolster their security architecture with Windows 11, while also improving update mechanisms, we hope to see a further reduction in both the number of vulnerabilities as well as in the windows of time during which they can be exploited in the wild. But with all the end-of-life operating systems still in production (reaching back to Windows XP), can the number of Windows vulnerabilities truly be expected to diminish much further? The simple answer to this riddle is yes, but the number will decrease for undesirable reasons.

In the future, Microsoft may not report or patch flaws on end-of-life products; however, new vulnerabilities may still exist on these end-of-life operating systems. End users may not know the vulnerabilities are present, or if there are any mitigating controls, and this creates an unnecessary risk blind spot.

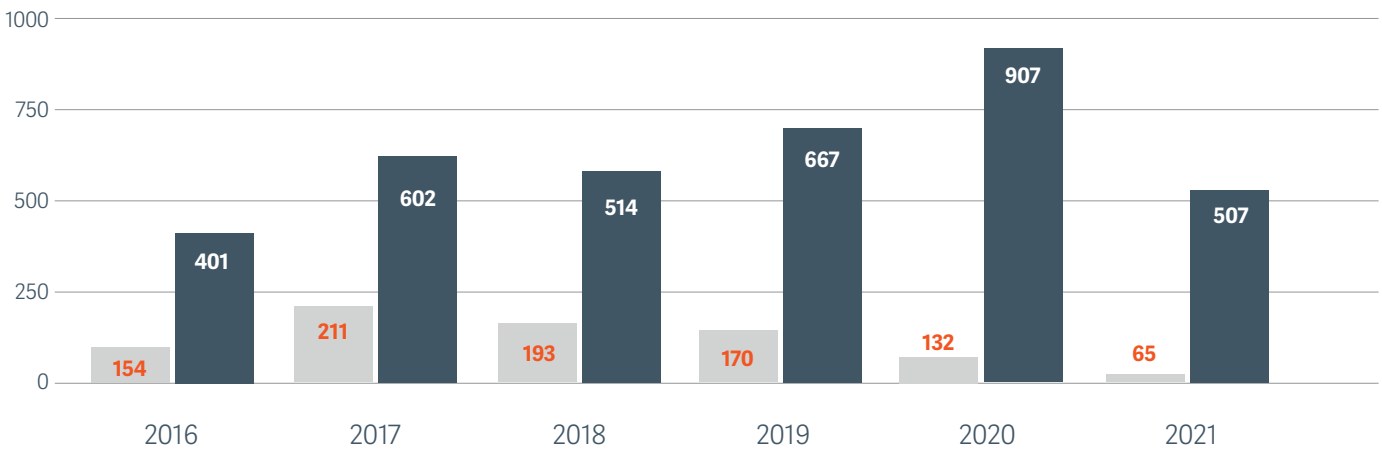
Microsoft will continue to document and report on vulnerabilities for supported solutions, and improved coding and security controls may lead to a decrease in vulnerabilities. Conversely, end-of-life solutions that are still supported could continue to serve as grounds for large numbers of new vulnerabilities.



The halving of Critical Windows vulnerabilities over the past five years is a positive development and reflects how the continued investment in building a more secure operating system is paying off for Microsoft and for Windows users.

Microsoft's more aggressive stance on updating Windows is also translating into a reduction in the amount of time systems are exposed to the risk of vulnerabilities. This two-punch combo of fewer vulnerabilities and faster patching comes as welcome progress after the relentless pressures of 2020.

Windows Vulnerabilities (2016 - 2021)



Microsoft Office Vulnerabilities

Microsoft Office (versions 2010, 2013, 2016, 2019) have seen a steady decline in Critical vulnerabilities over the past five years.

66 Total Microsoft Office vulnerabilities in 2021

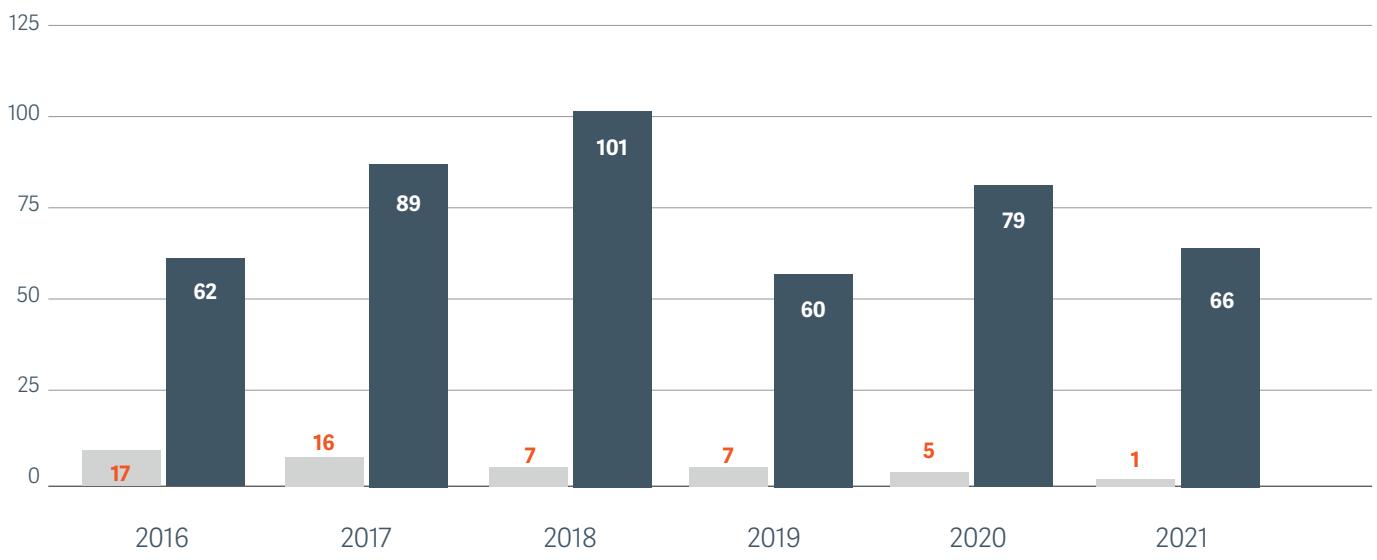
1 Only 1 was a Critical vulnerability

2021 saw 66 total vulnerabilities across Office products, but only 1 was considered Critical.

The reduction in total vulnerabilities, and almost complete elimination of Critical vulnerabilities, is most definitely welcomed when it comes to Microsoft's powerhouse application. However, there is a long tail of vulnerabilities still actively exploited by threat actors. CVE-2017-11882 (also known as the Equation Editor bug) was leveraged by numerous threat actors in 2021, despite a fix being available since November 2017. This bug allows an attacker to gain code execution, commonly exploited to install a Remote Access Tool (RAT).

Office applications are a common target for phishing campaigns. Yet, these applications are often not patched at as fast a cadence as the operating system by some organizations. Many malware toolkits contain numerous Office exploits aggregated from the past 10 years, with the goal of finding an unpatched system. These toolkits and strategies have proven highly successful for many threat actors.

Microsoft Office Vulnerabilities (2016 - 2021)



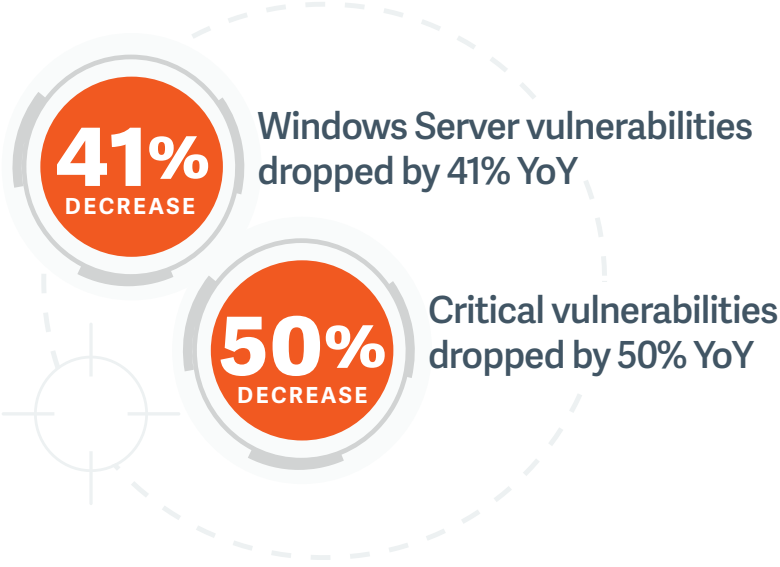
Windows Server Vulnerabilities

Microsoft has journeyed a long way since BeyondTrust CTO, Marc Maiffret, identified the Code Red Worm back in 2001, and was part of a team that consistently put pressure on Microsoft to improve their security practices and diligence in addressing vulnerabilities.

Before then, security was ostensibly an afterthought, and perhaps not considered at all unless it conspicuously threatened to affect revenue, business continuity, or market share.

It has taken Microsoft multiple generations of Windows Server to get to a version inherently more secure. The latest versions of Windows Server are a testament to threats that were identified over 20 years ago. The latest releases of Windows Server have fewer vulnerabilities than ever before, despite being some of the largest code bases for any operating system.

Windows Server vulnerabilities dropped to their lowest level since 2018, falling from 902 in 2020 to 531 in 2021 – a 41% reduction. Critical Windows Server vulnerabilities also dropped by 50% last year, hitting their lowest number since 2015.



Azure & Dynamics 365 Vulnerabilities

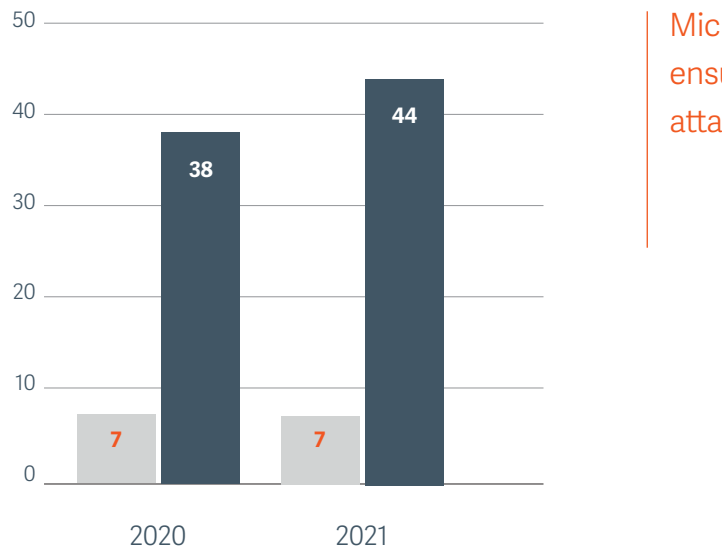
In 2014, in his first email to employees as new Microsoft CEO, Sattya Nadella espoused his vision of a mobile-first, cloud-first world, before publicly staking that vision.

Delivering quality and secure code in the cloud has been a longstanding priority for Microsoft.

If we consider the potential diverse implementations of Azure and Dynamics 365, then even basic misconfigurations could cause a vulnerability or weakness. Microsoft has taken impressive steps to ensure that vulnerabilities are not the primary attack vector for these cloud solutions.

Vulnerabilities in Azure and Dynamics 365 remained consistently low for the last couple of years. In 2021, Azure accounted for 30 vulnerabilities overall, and 5 Critical vulnerabilities. In 2020, Dynamics 365 accounted for 6 Critical vulnerabilities, but this dropped to only 2 last year.

Azure & Dynamics 365 Vulnerabilities (2016 - 2021)



Microsoft has taken impressive steps to ensure that vulnerabilities are not the primary attack vector for Azure and Dynamics 365.

Microsoft Vulnerabilities Decrease, But Caveats and Caution Apply

For the first time since this report began nine years ago, the total number of reported vulnerabilities in Microsoft products and platforms decreased (by 5%).

Since 2016, we had seen a steady rise in Microsoft vulnerabilities. With the world wracked and dramatically altered by the onset of a pandemic, 2020 represented a high watermark, to date, for the number of Microsoft vulnerabilities.

The number of Microsoft vulnerabilities soared by the highest percentage increase ever from 2019 to 2020. In 2021, the total number of vulnerabilities pulled back slightly from the 2020 highs, yet the overall vulnerability picture is mixed.

For the second consecutive year and second time ever, Elevation of Privilege (EoP) is the category with the most vulnerabilities recorded. From 2013 through 2019, Remote Code Execution (RCE) vulnerabilities accounted for the majority of recorded vulnerabilities annually.

The abrupt and persistent increase in EoP vulnerabilities across two reporting years is likely owed to multiple factors.

The new CVSS format has impacted visibility into how removing admin rights could have mitigated 2021's Critical vulnerabilities, due to the lack of Executive Summary information that Microsoft had historically been providing on vulnerabilities through 2020.

With that said, based off our understanding of the Microsoft landscape and previous trends, we estimate removing admin rights and enforcing least privilege remains pivotal to addressing vulnerabilities and reducing the attack surface.

Patching vulnerabilities is not always straightforward, or even desirable, based on an organization's environment, so removing admin rights is a best practice that can provide strong baseline security by reducing the attack surface. In addition to compliance initiatives, removing admin rights is now often specifically called out by cyber insurers, and is a control consistent with zero trust principles.

2015 - 2020 findings:
75% of Critical vulnerabilites
could have been mitigated by removing admin rights

7- IDSA study: 2021 Trends in Securing Digital Identities, IDSA, June 2021

High-Impact Vulnerabilities Spotlight

When examining the highest risks for remote code execution in 2021, we found some interesting differences from previous years.

Consider how the vulnerabilities detailed below, all with a CVSS score of 9.0+, have affected a wide variety of organizations:

CVE-2021-28480 and CVE-2021-28481

Microsoft Exchange Server Remote Code Execution Vulnerability

These two CVEs are for pre-authentication vulnerabilities in a Microsoft Exchange Server. A pre-authentication vulnerability means an attacker does not need to authenticate to the vulnerable Exchange Server to exploit the vulnerability. This was well-documented by Tenable.

To exploit these vulnerabilities, a threat actor performs reconnaissance against their intended targets and then sends specially crafted requests to exploit the server, assuming they have access on-premises, or the server is hosted on the Internet. These vulnerabilities served as a wake-up call to many organizations and accelerated moves to migrate from on-premises Exchange to Microsoft 365 in the cloud.

CVE-2021-34473, CVE-2021-26894, CVE-2021-26895, and CVE-2021-26897

Windows DNS Server Remote Code Execution Vulnerability

These four vulnerabilities are exploitable on Microsoft Windows servers that provide DNS services. Exploiting these vulnerabilities requires no authentication to completely compromise the host.

For a DNS server to be susceptible, dynamic updates must be enabled. Any organization providing DNS services to their infrastructure could be vulnerable. Due to the severity of these vulnerabilities, organizations should have immediately patched them.

8- 2021 Trends in Securing Digital Identities. IDSA. June 2021.

CVE-2021-42311 and CVE-2021-42313

Microsoft Defender for IoT Remote Code Execution Vulnerability

While these vulnerabilities are targeted at Microsoft's security solution for IoT (Internet of Things) assets, the exploitation of a security solution could be performed on-premises or in the cloud.

Both vulnerabilities are based on SQL injection. If exploited, these vulnerabilities allow a remote attacker to achieve arbitrary code execution, without authentication.

As documented by SentinelOne and SecurityWeek, it's possible to execute code with root privileges, if properly scripted. This one flaw alone demonstrates that privileged escalation attacks still indeed exist, but are not being reported on any longer by Microsoft in an easily accessible or quantifiable manner.

Most of the high-impact vulnerabilities detailed above also highlight the risks of on-premises technology and indicate that a shift to the cloud can improve an organization's security.

For further reading, this CSO Online article contains some valuable information and additional perspective around specific Microsoft vulnerabilities in 2021.

What Do the Experts Say?

Sami Laiho
Senior Technical Fellow, MVP

Russell Smith
Editorial Director, Petri IT Knowledgebase

Paula Januszkiewicz
Security Expert & Penetration Tester

James Maude
Lead Cyber Security Researcher, BeyondTrust

Morey Haber
Chief Security Officer,

Senior Technical Fellow, MVP
samilaiho.com
@samilaiho Twitter

Sami Laiho

It seems that we've reached some sort of steadier level again, when it comes to the amount of vulnerabilities found in a year. For both 2020 and 2021, we can say that we are at a steady pace of around 100 Microsoft vulnerabilities per month. Although we can see a decrease in the number of vulnerabilities for the first time in years, it's only -5%, and I don't really see this as a big change or anything to be too happy about. With Microsoft's move to the Common Vulnerability Scoring System (CVSS), it's not as easy to identify which vulnerabilities would have been mitigated by removing admin rights, but we can still see that one out of two vulnerabilities did aim at elevating privileges. So, because that is the one thing that the enemy wants, I'm still considering it as the most important thing to deny them.

I've done hundreds of big projects on this, removing more than 1 million local admins from companies, and the results speak for themselves. Many people see this as a "Big Brother is watching" annoying security feature that just tries to make working harder. What I see is that the most effective approach is to talk more about the benefits of removing admin rights, especially when it comes to productivity. I have customers who saw 75% fewer Service Desk tickets after removing admin rights. Computers just work better when you don't have privileges to break them.

> "The benefits of Least Privilege are so huge that I've kept away from logging into my own computers as admin for exactly 20 years today."

I also have a US customer who had 65% less reinstallations of computers after removing admin rights. One developer was very much against this, and the thing that won him over was the fact that I showed him that his SSD lives longer if he doesn't have admin rights. The benefits of Least Privilege are so huge that I've kept away from logging into my own computers as admin for exactly 20 years today. I would never go back, and neither would my kids, relatives, or customers.

Editorial Director,
Petri IT Knowledgebase

Russell Smith

Microsoft has traditionally been given a hard time by security professionals when it comes to vulnerabilities in its products, especially Windows and Office. But the data in this report shows Microsoft is successfully reducing the number of critical vulnerabilities across its flagship software products. And by quite a considerable margin.

That is no mean feat, considering Microsoft continues to support legacy functionality for enterprises, resulting in the largest codebase of any operating system. Bear in mind that Windows is installed on over a billion end-user devices, making it a prime target.

Because, unlike Linux-based servers, for example, there are also a billion sticky fingers that increase the likelihood of hackers compromising the OS using tactics like social engineering and phishing.

There has also been a fundamental shift over the past few years, with Microsoft offering security solutions for its own products. Microsoft's security business grew from $10bn to $15bn in just one year between 2021 and 2022. Microsoft 365 Defender, Azure Sentinel, and improvements in Windows and Office are among just some of the investments Microsoft has been making in security.

The shift to remote working has also changed how organizations manage Windows. Microsoft Intune, Endpoint Manager, and Windows Autopilot have all seen significant investment. These services enable businesses to deploy and manage remote devices more effectively.

Recently announced services, like Windows Autopatch for Enterprise E3 customers, will allow organizations to hand over security functions that Microsoft can manage more effectively using advanced technologies like machine learning.

Despite all the great work Microsoft is doing to improve security, Windows will remain a sitting duck because of its omnipresence in the enterprise space. And to help address the high prevalence of vulnerabilities, Microsoft is making it easier for organizations to manage use of administrative privileges in Windows, a first in the history of the company.

> "The data in this report shows Microsoft is successfully reducing the number of critical vulnerabilities across its flagship software products, and by quite a considerable margin."

It's a welcome and long overdue change. Elevation rules will require devices be managed by Microsoft's Mobile Device Management (MDM) platform, Intune. The options for controlling administrative privilege use will be limited compared to third-party solutions.

But as stated earlier in this report, it is critical that organizations continue to carefully manage administrative privilege use to protect against vulnerabilities in Microsoft's software. I've always been a strong advocate for limiting access to admin rights. But despite the importance of running with standard user privileges for protecting systems and data, it is still not possible to natively manage in Windows today. Organizations need to manage privileged access on endpoints in a flexible and secure way that reduces risks to the business while allowing employees to do their work.

BeyondTrust continues to provide the best solution for enabling that fine balance between security and usability in Windows.

Security Expert &
Penetration Tester
@PaulaCqure Twitter

Paula Januszkiewicz

On April 8, 2014, Microsoft officially announced the end of support for the Windows XP operating system. January 14, 2020 was supposed to be the end of Windows 7, as Microsoft also announced the end of support for that operating system. In reality, both systems are alive.

It is nothing unusual to find end-of-support operating systems across the globe, operational in critical infrastructure as well as in health care facilities. According to Kaspersky's survey from 2021, almost one quarter (24%) of PC users are still running a Windows OS without mainstream support.

There is a big problem, especially with operational technology (OT). It is designed to have a much longer lifespan than IT systems. OT systems are much more likely to include components that are 20-30 years old, or even older. Very often, security patches are not applied in OT systems. This is because these systems are expected to be operated with minimal interruptions. Updates, such as patches, may be considered as something that interferes with business continuity.

A few years back, this hesitance to patch OT systems was not a big issue because many industrial control systems (and human-machine interfaces used with them) were designed for isolated environments. In the last few years, especially after the introduction of pandemic measures, connectivity between OT and IT networks has been growing rapidly. This makes OT systems exposed on the internet.

> "Known and new vulnerabilities could put critical infrastructure in danger, as the distinction between IT and OT systems is becoming increasingly blurred."

Critical infrastructure is no longer in the safe bubble. And, by using outdated operating systems without support, this infrastructure is in an extremely dangerous position. Attackers have easy access to publicly available exploits and can deploy them anytime. Known and new vulnerabilities could put critical infrastructure in danger. Distinction between IT and OT systems is becoming increasingly blurred.

I'm happy to see that Microsoft vulnerabilities dropped by 5% in 2021. But in the rapidly changing world, it is amazingly easy to forget about those lagging behind, and as a result, we can pay a high price for this.

EXPERT COMMENTARY

Chief Security Officer,
BeyondTrust

Morey J. Haber

As the Chief Security Officer for a leading cybersecurity organization like BeyondTrust, I can say that we license security solutions just like any other company. And while my employees and assets are customer number one for the solutions we develop, no security vendor creates all the solutions required for a complete security stack. It's a fact that every company must license some technology from someone else.

As a security best practice, a risk assessment helps document the threats to an organization. Internal business practices then rank identified risks. Internally, my organization (like many other businesses) decides which ones to prioritize, which ones require operational changes, and which ones require remediation. While critical vulnerabilities are always remediated first, the fact that some vulnerabilities require privileges to be exploited surfaces as a trend that can be resolved using a long-term mitigation strategy – least privilege operations.

We are a client of our own solutions. The removal and management of administrator rights on every asset, and for every user, is an important mitigation strategy for us. If you remove and manage administrative privileges, the risk surface for high and critical vulnerabilities almost always decreases (except for exploits that have privileged escalation as a part of their attack vector). This is because exploits that require privileges can no longer operate.

As a CSO, and for many of my peers, we are always looking for the most efficient way to mitigate risk. Sometimes the answer is changing processes, developing policy, modifying configurations, or licensing a technology to manage the threat.

"If you remove and manage administrative privileges, the risk surface for high and critical vulnerabilities almost always decreases."

As the risk of critical vulnerabilities continues to threaten businesses every year, we have learned applying patches in a timely manner is crucial to managing the problem. However, efficiency is more than a finely tuned process of vulnerability and patch management. Getting ahead of the problem is a part of efficiency. Mitigating the risks by implementing least privilege across the enterprise is a first step to solving the long-term problem.

Any steps an organization can take to get ahead of the "scan and patch" mentality will help offset the risk from the onslaught of vulnerabilities year after year. Removing and managing administrative privileges, we have found, is the most effective change any organization can make.

EXPERT COMMENTARY

Lead Cyber Security Researcher, BeyondTrust

James Maude

It has been 20 years since Bill Gates launched Microsoft's "Trustworthy Computing" memo that set out a vision for prioritizing security over adding new features. The intention of the memo was to put customer security and trust at the forefront of employees' minds and rebuild the company's reputation.

"Eventually, our software should be so fundamentally secure that customers never even worry about it."
- Bill Gates, Trustworthy Computing Memo, 2002

There is also a personal connection here at BeyondTrust. A year prior to the memo, a young researcher named Marc Maiffret (now CTO of BeyondTrust) discovered the Code Red worm, which exploited a vulnerability in Microsoft IIS web servers. This and other vulnerabilities shook customer confidence and caused some soul searching at Microsoft - leading to secure coding practices and the famous memo.

This set in motion a chain of events that led to the consolidation of Microsoft's security update process, with the first Patch Tuesday the following year. This not only provided visibility and accountability for customers, but also the data that we have used in this report for the past 9 years.

While it is easy to look back and cynically say that not a lot has changed as we are still seeing new vulnerabilities, I think this report is a testament to how far things have progressed.

Let's start with the reporting format itself. The new format of the Security Update Guide shows that Microsoft is serious in committing to industry standards with the Common Vulnerability Scoring System (CVSS). This allows Microsoft vulnerabilities to be captured and scored in a standard way alongside any other vendor. Not only does this improve transparency, but it also makes it easier for organizations to assess and prioritize their vulnerability management.

> "No longer can attackers assume a user has local admin rights or a process is running with privileges. This reinforces why the basic principle of least privilege, combined with software patching, are the foundations of any security program."

As we dig into the data this year, we can see the continuing downward trend in critical vulnerabilities. This is not simply good luck either - it represents the investment put into security by Microsoft. Put simply, this investment has made it significantly harder for an attacker to leap from a browser vulnerability to total control of the system in one move. This is borne out in the wider data set with attackers being forced to try and chain multiple vulnerabilities together, leading to an overall increase in vulnerabilities, but a decrease in overall severity.

Finally, the rise of Elevation of Privilege attacks might tell the story that privileges aren't as available to attackers as they used to be. No longer can they assume a user has local administrator rights, or if a process is running with privileges. This also reinforces why the basic principle of least privilege, combined with software patching, are the foundations of any security program.

As for the memo, lets see if we are *"so fundamentally secure that customers never even worry about it"* in another 20 years!

Mitigating Microsoft-Based Vulnerability Risks

In a world of stolen identities, phished passwords, and deepfakes, simply trusting users and systems is ***not enough.***

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

When it comes to reducing the risk associated with admin rights and Microsoft's Critical vulnerabilities, our Endpoint Privilege Management solution is a best-in-class solution and delivers a robust range of benefits.

With Endpoint Privilege Management you can:

1. **Remove excessive end-user privileges** on Windows, Mac, Unix, Linux, and network devices.

2. **Quickly implement least privilege** by eliminating local admin rights across all endpoints and achieve rapid leaps in risk reduction via out-of-the-box Quick Start policies.

3. **Protect against phishing, ransomware, and malware threats** and reduce attack surfaces by assigning just-in-time (JIT) privileges only to approved applications, scripts, tasks, and commands that require them.

4. **Address compliance needs** by removing excess privileges, using application whitelisting, and providing an audit trail of user activity.

5. **Qualify for cyber insurance** by removing admin rights, enforcing least privilege, controlling applications, and applying other security controls demanded by cyber insurers.

The BeyondTrust Platform

Privileged Password Management solutions enable automated discovery and onboarding of all privileged accounts, secure access to privileged credentials and secrets, and auditing of all privileged activities.

Endpoint Privilege Management solutions combine privilege management and application control to efficiently manage admin rights on Windows, Mac, Unix, Linux, and network devices, without hindering productivity.

Secure Remote Access solutions enable organizations to apply least privilege and robust audit controls to all remote access required by employees, vendors, and service desks.

Cloud Security Management solutions help organizations pinpoint and mitigate risks associated with cloud access permissions and entitlements across multicloud environments.

ON-PREMISES CLOUD HYBRID

Beyondinsight Discovery | Reporting | Threat Analytics | Connectors | Central Policy & Management

Conclusion

Regulations, compliance standards, security best practices, and even, increasingly, cyber insurance providers, all dictate that we need to identify and appropriately address the latest threats. Analyzing the threat landscape every year can also help your organization become more efficient at solving the problem. However, implementing an efficient process to effectively address threats and eliminate or mitigate vulnerabilities in a timely manner is an entirely different problem.

Key Considerations for Achieving Cybersecurity Goals

Executive Sponsorship

The executive leadership must be fully on board with the implementation of a risk mitigation process. While the cost of the program may always be a concern, the executive team must weigh that against the potential risk – both financial and reputational.

Better yet, they should grasp the business-enabling benefits of such an implementation, such as the ability to confidently embrace or expand digital transformation technologies and initiatives.

Procedures and Policy

A risk management process needs to be designed with guidelines and service level agreements, including clear lines of ownership. This workflow should be documented, reviewed periodically, and followed to ensure remediation and mitigation strategies are effective.

Measurements and Consequences

One of the hallmark traits of a bad risk mitigation process is complacency accompanied by a lack of accountability. In addition to procedures and policies, define clear project ownership, key metrics across the organization, and the consequences if those metrics are not met.

Basic Security Hygiene

If you do the basics well—such as vulnerability assessments, patch management, systems hardening, and privilege access management—you will not only have a strong baseline security posture, but you will also find flaws in your organization quicker and will be able to address them more effectively.

Finally, when you consider the risks your organization may face, consider PAM capabilities—including least privilege enforcement and secure remote access—to be core tenets for threat mitigation and attack surface reduction. Most exploits—whether run-of-the-mill malware, ransomware, or advanced persistent threats—need administrative privileges to execute. The elimination of unnecessary admin rights can prevent a bad situation from becoming worse; years of data support this approach.

When you review the trends in this report and today's threat landscape, it's important to acknowledge it is essential to build an effective preventative and proactive security posture—one that goes far beyond reactive defenses, such as vulnerability and patch management.

Methodology

The BeyondTrust Microsoft Vulnerabilities Report, produced annually, analyzes the data from security bulletins issued by Microsoft throughout the previous year. This report compiles these security releases into a year-long overview, presenting a holistic view of trends related to vulnerabilities, with insights on vulnerability mitigation.

In November 2020, Microsoft introduced their new Common Vulnerability Scoring System (CVSS) reporting format. With this reporting change, executive summaries for individual Microsoft vulnerabilities were no longer provided by Microsoft. Without this executive summary information, a clear determination cannot be made about the number of Microsoft vulnerabilities that could have been mitigated if admin rights had been removed. This change has not impacted the ability to report on vulnerability volume by product and platforms.

How Microsoft Classifies Vulnerabilities

Each vulnerability can apply to one or more Microsoft products. This is shown as a matrix on each vulnerability page. Each vulnerability is assigned a type from one of seven categories: Remote Code Execution, Elevation of Privilege, Information Disclosure, Denial of Service, Security Feature Bypass, Spoofing, and Tampering– which occasionally vary depending on the individual piece of software or combination of software affected. A vulnerability of each type often applies to a combination of different versions of a product or products, and sometimes all versions – e.g. all versions of Windows clients. Often, a vulnerability will only apply to a combination of products – e.g. Internet Explorer 11 on Windows 7.

Each vulnerability is also assigned an aggregate severity rating by Microsoft – Critical, Important, Moderate – which varies depending on each individual piece of software, or combination of software affected. Certain vulnerabilities have occurred multiple times throughout 2021, usually affecting different software. In these cases, the vulnerability itself is only counted once, with all affected software types attributed to that one entry.

Accuracy of Vulnerability Data
Several generalizations have been made for each vulnerability as follows:

1. Each vulnerability was classified with the highest severity rating of all instances of that vulnerability where it appeared multiple times
2. Each vulnerability was classified with the most prevalent type for all instances of that vulnerability
3. Product versions were not taken into account
4. Product combinations were not taken into account
5. Vulnerabilities were counted for both the software and version where appropriate (for example, a vulnerability for Internet Explorer 11 on Windows 10 is taken as a vulnerability for both Internet Explorer 11 and Windows 10

Additonal Resources

NEW! Privileged Access Discovery Application
Illuminate privileged access risk with the most powerful free tool of its kind. Scan your environment and pinpoint overprivileged accounts, service accounts, unused accounts, privileged credentials, remote access tools, and more.

WHITEPAPER Cybersecurity Survival Guide

WHITEPAPER Malware Threat Report 2021

WHITEPAPER The 7 Perils of Privilege

BeyondTrust

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