WHITE PAPER

MICROSOFT VULNERABILITIES REPORT 2020

Discover the dangers of unmanaged admin rights & strategies to control them

BeyondTrust

TABLE OF CONTENTS

1 Introduction & Executive Summary 3

2 Data Highlights 5

3 Vulnerabilities by Product 6

- Internet Explorer & Edge 6
- Windows 7
- Windows Office 8
- Windows Server 9

4 The Big Picture: Five Year View 10

5 Expert Commentaries 11

- Jane Frankland, Cybersecurity Expert 11
- Paula Januszkiewicz, CQURE CEO 12
- Sami Laiho, Microsoft MVP & Ethical Hacker 13

6 BeyondTrust Endpoint Privilege Management 14

7 Achieving Compliance 14

8 Next Steps & Resources 15

9 Methodology 16

- How Microsoft Classifies Vulnerabilities 16
- Accuracy of Vulnerability Data 17

1 Introduction & Executive Summary

The BeyondTrust Microsoft Vulnerabilities Report, produced annually, analyzes the data from security bulletins issued by Microsoft throughout the previous year. Every Tuesday, Microsoft releases fixes for all vulnerabilities affecting Microsoft products, and this report compiles these releases into a year-long overview, creating a holistic view of trends related to vulnerabilities and, more importantly, how many Microsoft vulnerabilities could be mitigated if admin rights were removed from organizations.

This is the 7th annual edition of the Microsoft Vulnerabilities Report, and includes a five-year trend comparison, giving you a better understanding of how vulnerabilities are growing and in which specific products.

Executive Summary

Below are some of the key findings from this year's Microsoft Vulnerabilities Report, which analyzes all Patch Tuesday bulletins released throughout 2019.

- In 2019, a record high number of **858 Microsoft vulnerabilities** was discovered
- The number of reported vulnerabilities has **risen 64% in the last 5 years** (2015-2019)
- Removing admin rights would **mitigate 77% of all Critical Microsoft vulnerabilities** in 2019
- **100% of Critical vulnerabilities** in Internet Explorer & Edge would have been mitigated by removing admin rights
- **80% of Critical vulnerabilities** affecting Windows 7, 8.1 and 10 would have been mitigated by removing of admin rights

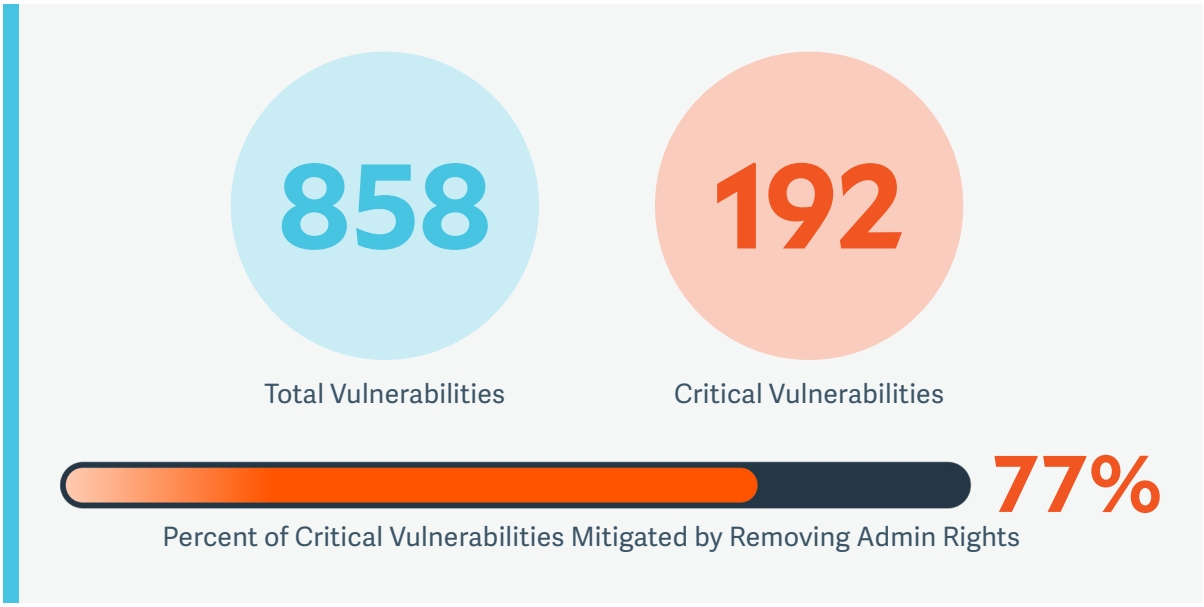


Figure 1: Microsoft Vulnerability Statistics (2019)

How Microsoft Groups Vulnerabilities

Each Microsoft Security Bulletin comprises of one or more vulnerabilities, applying to one or more Microsoft products. These categories, organized by impact type, consist of Remote Code Execution, Elevation of Privilege, Information Disclosure, Denial of Service, Security Feature Bypass, Spoofing and Tampering.

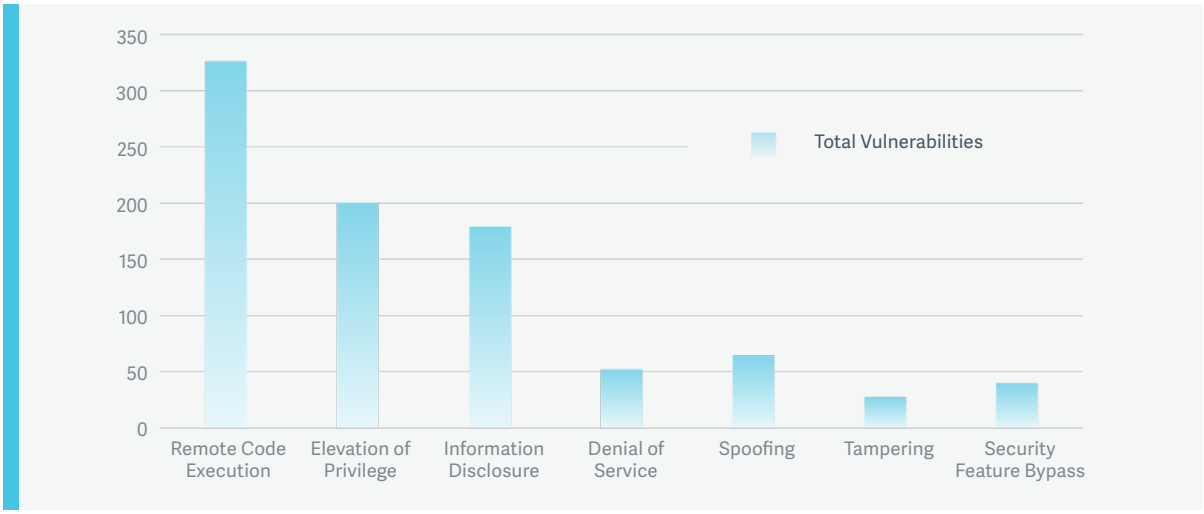


Figure 1: Breakdown of Microsoft Vulnerability Categories (2019)

Remote Code Execution (RCE) vulnerabilities in 2019 hit a record high, while Elevation of Privilege vulnerabilities also rose by 37% since last year

As per previous reports, Remote Code Execution (RCE) account for the largest proportion of total Microsoft vulnerabilities throughout 2019. Of the 323 RCE vulnerabilities, 191 were considered Critical. Of these Critical vulnerabilities, the removal of admin rights would have mitigated 76%. RCE vulnerabilities in 2019 hit a record high, while Elevation of Privilege vulnerabilities also rose by 37% since last year.

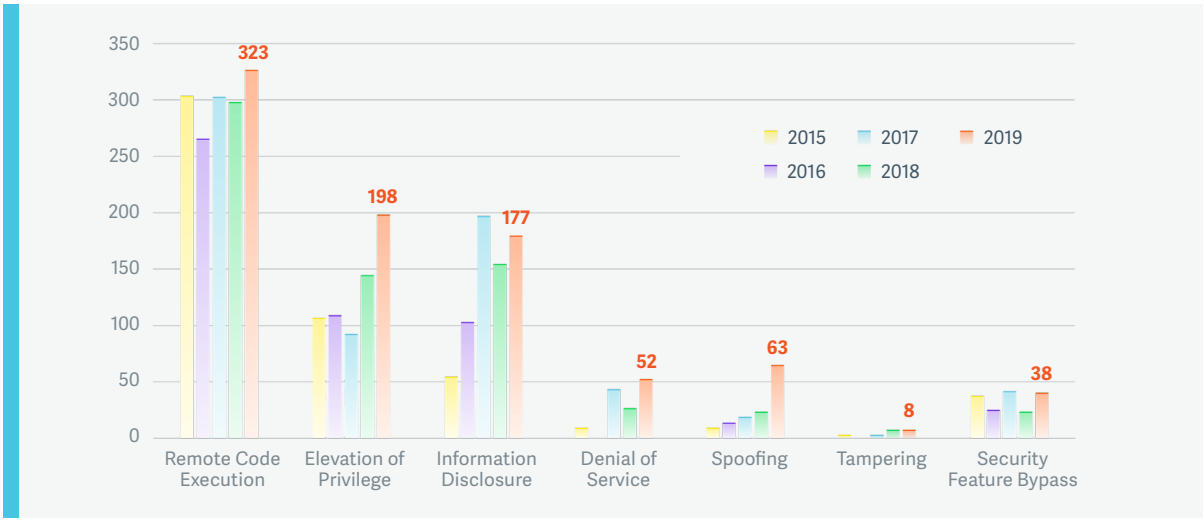


Figure 2: Vulnerability Categories (2015-2019)

2

2019 Data Highlights

In 2019, Microsoft reported a **record high** number of vulnerabilities.

858

Total Vulnerabilities

64%

5 Year Average Increase

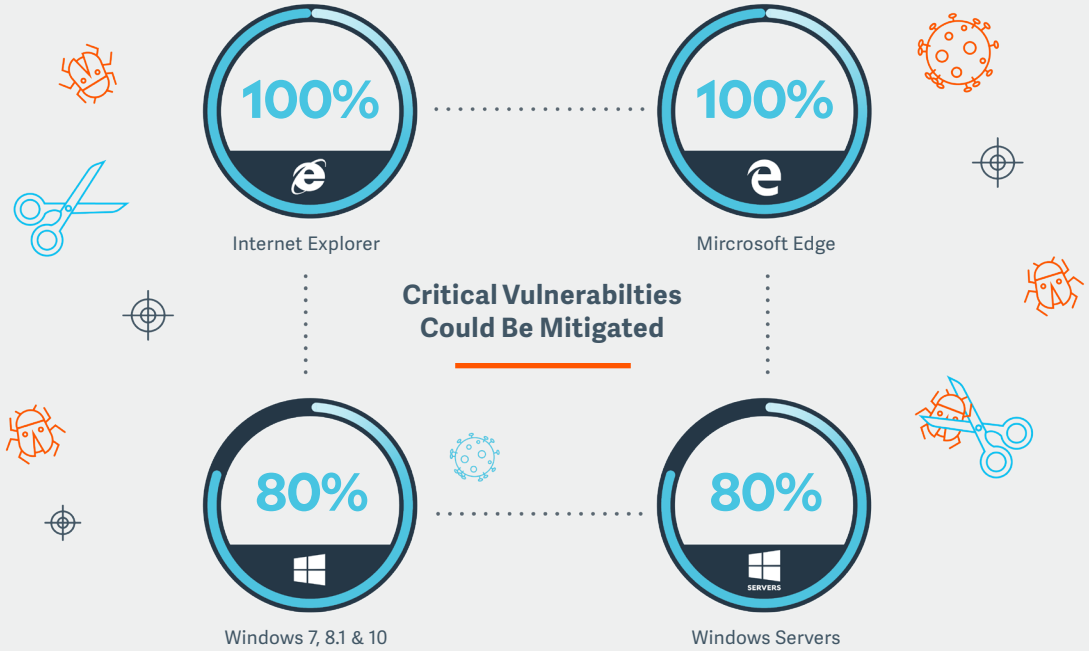
Reported Vulnerabilities have jumped from 524 (2015) to 858 (2019)

77%

Critical Vulnerabilties Could Be Mitigated

The removal of admin rights could have significantly reduced the risks

How would removing **admin rights** help for key products?



3

Vulnerabilities by Product

INTERNET EXPLORER & EDGE

Despite the dominance of Google Chrome and Firefox, Microsoft Internet Explorer is still a very popular browser, yet since January 2016 Microsoft only supports and patches the most current version of Internet Explorer available for a supported operating system. It's worth noting that Microsoft Internet Explorer (IE) 10 reached end of support on January 31, 2020. From that point forward, IE 11 became the only supported version of Internet Explorer on Windows Server 2012 and Windows Embedded 8 Standard.

Removing admin rights could have mitigated 100% of the risk.

There were 33 Critical vulnerabilities discovered across Internet Explorer 8, 9, 10 and 11 during 2019. Removing admin rights could have mitigated 100% of the risk.

Critical vulnerabilities in Microsoft Edge have increased significantly since its inception two years ago, with 86 discovered last year. Of those 86, removing admin rights could have again mitigated 100% of the risk.

On January 15, 2020, Edge moved to a Chromium-based engine, meaning that both Google Chrome and Edge could have the same flaws at the same time, leaving no "safe" mainstream browser to use as a mitigation strategy to Edge vulnerabilities.

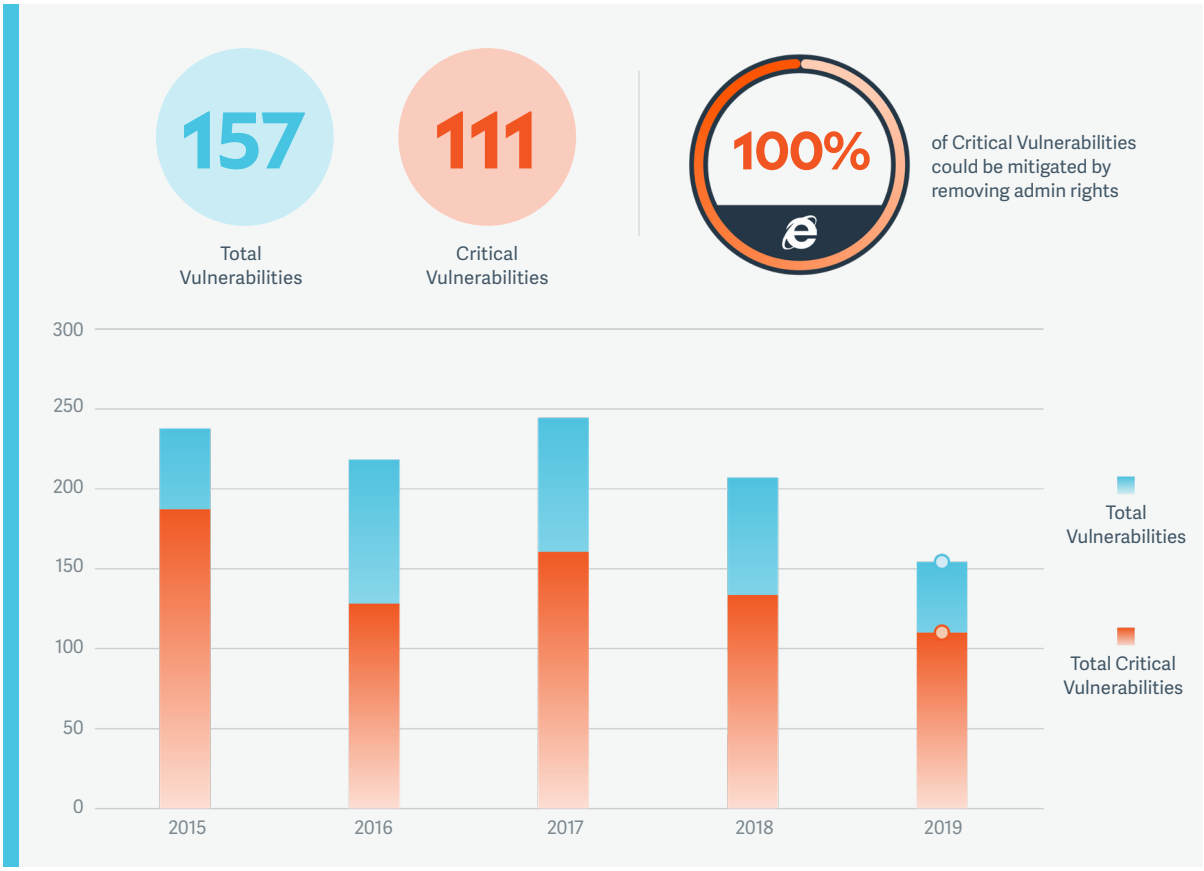


Figure 4: Microsoft Internet Explorer & Edge Vulnerabilities (2015-2019)

Windows 10 was touted as the "most secure Windows OS" to date when it was released, yet it still experienced 167 Critical vulnerabilities last year.

WINDOWS

In 2019, 667 vulnerabilities were reported across Windows Vista, Windows 7, Windows RT, Windows 8/8.1, and Windows 10 operating systems. Windows 10 was touted as the "most secure Windows OS" to date when it was released, yet it still experienced 167 Critical vulnerabilities last year. Of all the Windows vulnerabilities discovered in 2019, 170 were considered Critical.

Removing admin rights could have mitigated 80% of these critical vulnerabilities.

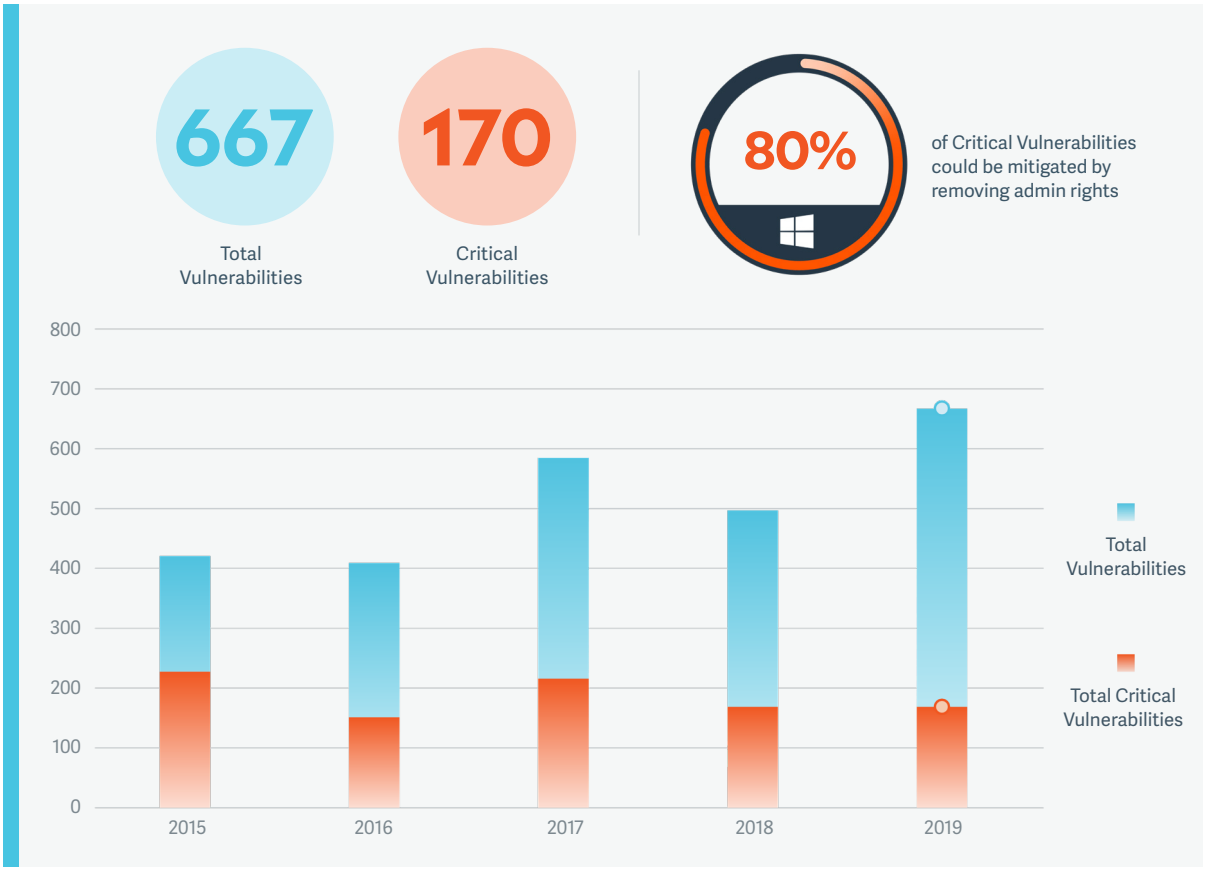


Figure 5: Microsoft Windows Vulnerabilities (2015-2019)

"Prevention techniques like application whitelisting, removing administrative access, and adopting the principles of least privilege go a long way toward protecting individual users' machines and reducing inroads to the network, while not severely restricting user functionality."

Dr. Eric Cole, Founder & CEO of Secure Anchor Consulting

WINDOWS OFFICE

After hitting a record high of 102 vulnerabilities in 2019, Office saw a dip this year, as they almost halved (60). Of the 60, only 7 were considered Critical and removing admin rights would mitigate 100% of them in all Office products in 2019 (Excel, Word, PowerPoint, Visio, Publisher and others).

Figure 6: Windows Critical Vulnerabilities (2015-2019)

WINDOWS SERVER

A total of 668 vulnerabilities were reported in Microsoft Security Bulletins affecting Microsoft Windows Server in 2019. Of the 171 vulnerabilities with a critical rating, 79% could be mitigated by the removal of admin rights.

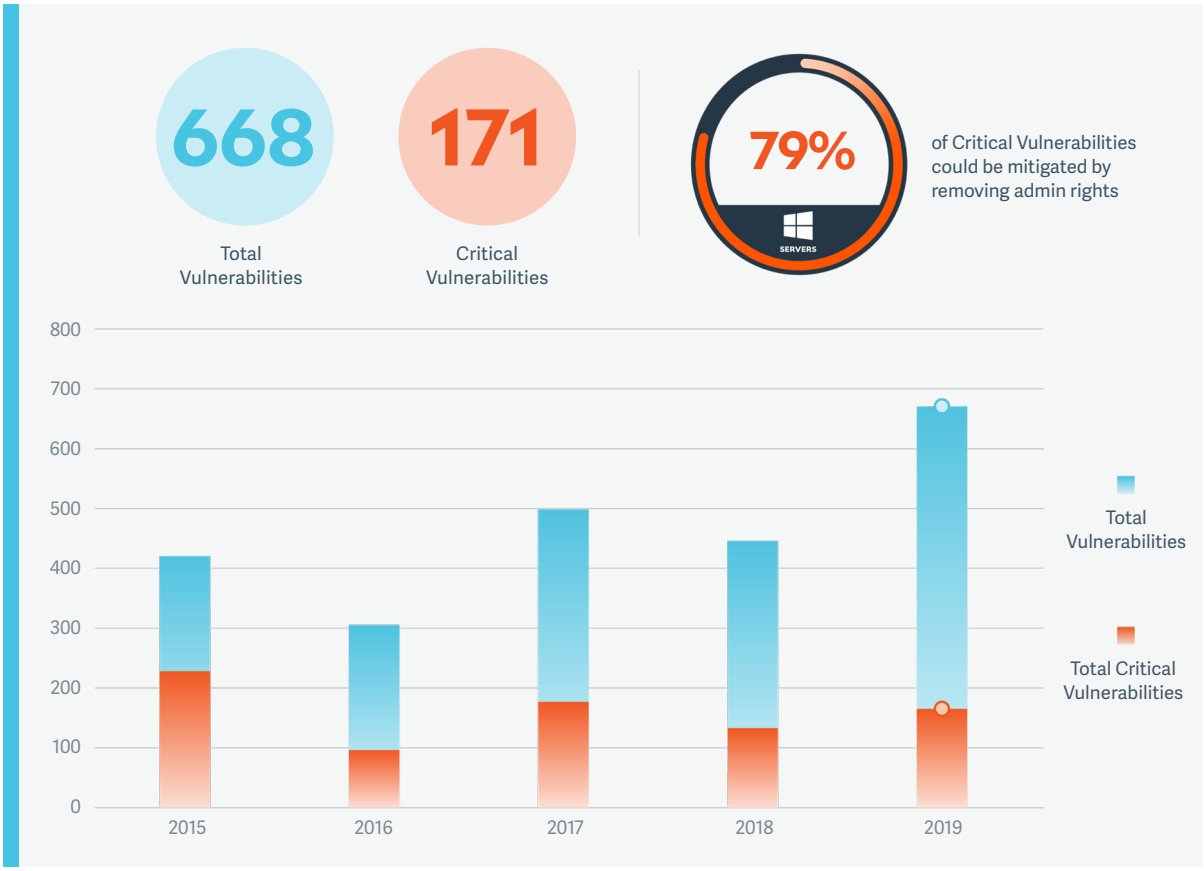


Figure 7: Windows Server Vulnerabilities (2015-2019)

In 2013, 252 vulnerabilities in Microsoft Windows Server were found – meaning that there has been a significant rise in vulnerabilities over the last six years.

4
The Big Picture: Five Year View

Critical vulnerabilities continue to introduce risk and create significant concern for organizations committed to protecting their networks from data breaches. The analysis in this report indicates that most of these vulnerabilities can be mitigated by the removal of local administrator rights.

Critical vulnerabilities continue to introduce risk and create significant concern for organizations committed to protecting their networks from data breaches.

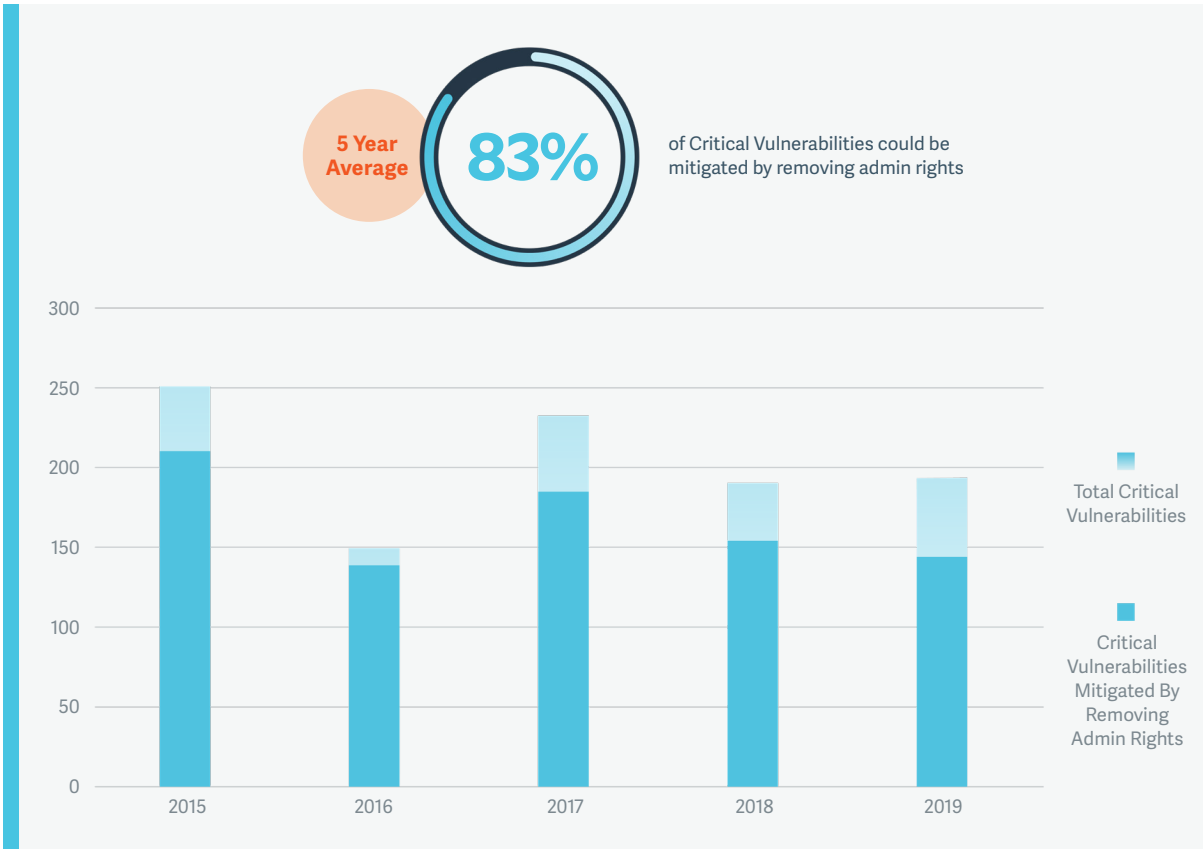


Figure 8: Microsoft Critical Vulnerabilities (2015-2019)

5 Expert Commentaries

JANE FRANKLAND

Author of IN Security & Award-winning Cybersecurity Speaker

The amount of data we produce and share is growing exponentially and the security infrastructure that safeguards this data is coming under increasing stress. With a growing attack surface coupled with a skills shortage, attacks are rising in volume and quality. Being persistent and complex, the speed and intensity of these attacks continue to challenge every part of our ecosystem. BeyondTrust's report clearly demonstrates this and it comes as no surprise to see vulnerabilities rising so significantly.

Whether it's adversaries who are in search of weak points, or employees who accidentally jeopardize the organization through insecure practices, people have historically been regarded as the weakest link. That's why virtually all exploited vulnerabilities are now likely to be the ones known by security researchers and experts. Unpatched systems remain low hanging fruit for adversaries looking to breach a network and gain entry to an organization. Even after decades of campaigning, patching – a basic security practice – is still not being applied effectively. Although most organizations have processes in place to quickly deploy critical patches released from vendors at the time of an exploited vulnerability, many struggle with non-critical, routine patches. And it's this issue we must resolve. Successful patching reduces vulnerability exploitations, significant system outages, availability issues, financial losses and reputational risk.

> "Removing admin rights is one of the most basic, yet powerful and protective measures an organization can take.

To reduce threats considerably, organizations would be well advised to remove admin rights by default. Often, they're working unaware of external vulnerabilities that come from using insecure applications and operating systems. If these are discovered ahead of an adversary, for example, during a security assessment or by security researchers, then vulnerabilities can be patched. But if they're not, then it's usually only a matter of time before an adversary discovers them and it's game over.

Removing admin rights reduces internal risks that come from installations of malicious applications like spyware or malware, which exist to steal data and money, hijack systems and disrupt business. Removing admin rights can remove back-doors for third parties to do the same, and render sensitive data unavailable for accessing, modification or exportation. Users would also no longer be able to create changes and lock legitimate users out of systems or publish unauthorised content online that could cause damage to the brand. It's simply one of the most basic, yet powerful and protective measures an organization can take.

PAULA JANUSZKIEWICZ

Cybersecurity Expert & CEO of CQURE

Nowadays, social engineering techniques used to target individual users, such as sending a malicious email attachment, are commonly used methods to get access to the internal corporate networks. The BeyondTrust Microsoft Vulnerabilities Report shows this trend thoroughly – it seems that attackers focus on vulnerabilities in all the products that may be treated as points of entry to the company and that can be used to spread the malicious code.

The malicious attachment or link could be used to exploit the vulnerabilities in the Internet Explorer, Microsoft Edge or Microsoft Office applications. One bad decision – the user has opened that link or attachment – leads to the open access to the system.

Let's imagine that this user has local administrator privileges. In this case the attacker may have access not only to all files in the system that might be downloaded or encrypted, but there is also a great possibility to gather credentials – for instance from the LSASS – to use it to attack other machines in the network. If the user works with server or domain admin privileges, the attacker may get access to those critical hosts and services. This is also a perfect environment for ransomware – if users are operating with admin rights, the ransomware can spread more easily.

If the least privilege principle was well implemented and the user does not use admin privileges for daily work, the attacker would have to put in much more effort to escalate privileges and perform traversal movement to other machines.

Implementing the least privileged principle is one of the most important tasks that companies should do to protect themselves from the mentioned vulnerabilities.

> “ If users are operating with admin rights, the ransomware can spread more easily.

If users are operating with admin rights, the ransomware can spread more easily.

Elaborating the Privileged Access Management subject, it is also crucial to patch software and systems in order to remove all vulnerabilities that may be exploited.

Using features built into Windows 10 could also be helpful when it comes to minimizing the risk of the successful attack. Windows Defender Exploit Guard is able to hold off the exploitation of the vulnerabilities existing in the software by protecting the processes. Credential Guard could be used to isolate credentials operations with using the virtualization. Also whitelisting of applications that may run on the workstation may stop malicious code from being executed.

To conclude, all mitigations together may successfully reduce the risk of the successful attack.

SAMI LAIHO

Microsoft MVP & Ethical Hacker

The whopping 858 vulnerabilities in 2019 is so big that, although reactively patching operating systems and apps is as important as ever, there is more need for proactively protecting our environments. I believe that the best protection for environments is achieved by concepts like Principle of Least Privilege, Whitelisting, MFA and education/awareness.

On top of common malware, I see the biggest threats to my customers being ransomware and phishing. Most of the traditional malware can be mitigated by removing admin rights. The results are insanely good compared to reactive measures especially when looking at Office apps and browsers!

You should remember that removing admin rights is not just about security. Removing admin rights will also allow your computers to run faster, better and longer, with less reinstallations. My bigger customers have also measured 75% reduction in the amount of Helpdesk tickets after removing admin rights. This means you can be more secure and more productive for extended periods of time!

> “ Removing admin rights is not just about security - it will also allow your computers to run faster, better and longer.

Removing admin rights doesn't really solve the issue of ransomware although it helps to reduce it spreading. The problem is evident – You need write permissions to your data and therefore can also encrypt it. The best protection against Ransomware is whitelisting. Whitelisting kills ransomware at its entry points, like email and web browsers.

One of the most common threats nowadays is phishing. It's not something that can be solved with technical protections only, as it's difficult to make sure people don't type their passwords in the wrong places or reuse passwords in multiple services. The good news is that 99% of phishing attacks can be mitigated by implementing Multi-Factor Authentication (MFA). The tough last percent can only be fought against with training and increase of awareness and that's why simulated phishing attacks should be implemented in all enterprises combined with mandatory security training.

6 BeyondTrust Endpoint Privilege Management

The findings of this report show that a great number of risks can be easily mitigated if administrator rights were removed, a practice recommended by many industry experts as well. What barriers exist that prevent organizations from addressing this risk?

The right security solution can enable organizations to achieve least privilege with products that not only deploy quickly, but also strike the right balance between security and productivity.

Implementing least privilege for desktops and servers are critical steps along the path to Universal Privilege Management, the BeyondTrust model for enabling Privileged Access Management (PAM).

Implementing least privilege for desktops and servers are critical steps along the path to Universal Privilege Management, the BeyondTrust model for enabling Privileged Access Management (PAM). Endpoint Privilege Management is a core solution of the BeyondTrust PAM portfolio.

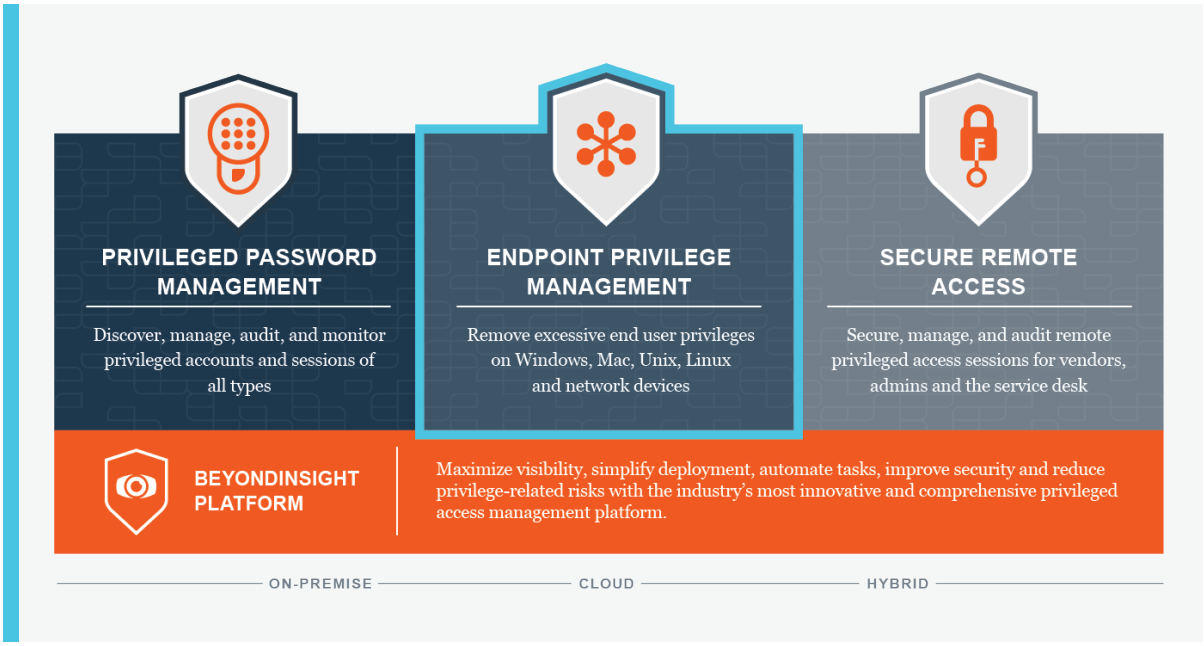


Figure 9: The BeyondTrust Solution Portfolio

With Endpoint Privilege Management, you can quickly remove excessive end user privileges on Windows, Mac, Unix, Linux and network devices, and achieve immediate risk reduction without impacting user productivity.

You can also meet internal and external compliance needs by removing excess privileges, using application whitelisting, and providing an audit trail of user activity.

> *Our Endpoint Privilege Management solution is available via virtual or physical appliance and in the Cloud (SaaS), so that organizations of all sizes can achieve endpoint security with a solution that is both scalable and cost-effective.*

7 Achieving Compliance

Implementing the principle of least privilege and removing administrator rights is a key requirement for many compliance mandates around the world. Compliance requirements can be banded into three primary purposes—**protect**, **control**, and **audit** the use of IT resources and the sensitive data they contain.

Deploying a comprehensive endpoint privilege management solution as part of your wider security strategy enables organizations to meet the following requirements:

- Track, control, prevent, and correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications. (CIS, PCI, NIST, HIPAA, GDPR)
- Implement only one primary function per server and enable only necessary service, protocols, daemons, etc. as required for the function of the system. (PCI, CIS)
- Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack; audit logs should specify user identification, type of event, date and time. (CIS, PCI, NIST, HIPAA, GDPR)

Find a complete list of these requirements and how BeyondTrust products enable them in the detailed Compliance Matrix.

8 Next Steps & Resources

By addressing unmanaged admin rights, you can quickly achieve endpoint security while eliminating security gaps and meeting compliance requirements, without hindering user productivity.

Contact BeyondTrust today to schedule a demo of Endpoint Privilege Management and view these additional resources.

Whitepaper

- A Comprehensive Guide to Endpoint Privilege Management

Case Study

- How the University of Derby Secure their Endpoints with BeyondTrust

Video

- A Two-Minute Overview of our Endpoint Privilege Management Solution

Datasheets

- Privilege Management for Windows & Mac
- Privilege Management for Unix & Linux

9 Methodology

Each bulletin issued by Microsoft contains an Executive Summary with general information. For this report, a vulnerability is classified as one that could be mitigated by removing admin rights if it meets the following criteria stated by Microsoft in the vulnerability bulletin:

- 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

HOW MICROSOFT CLASSIFIES VULNERABILITIES

Each vulnerability can apply to one or more Microsoft product. 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, Tampering– which occasionally vary depending on the individual piece 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 also varies depending on each individual piece of software, or combination of software affected. The Common Vulnerability Scoring System (CVSS is a published standard used by organizations worldwide and provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes.

Certain vulnerabilities have occurred multiple times throughout 2019, 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

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 Internet Explorer 11 on Windows 10 is taken as a vulnerability for both Internet Explorer 11 and Windows

ABOUT ENDPOINT PRIVILEGE MANAGEMENT

BeyondTrust Endpoint Privilege Management combines privilege management and application control to efficiently manage admin rights on Windows, Mac, Unix, Linux, and network devices without hindering productivity. Enforce least privilege and eliminate local admin rights with fine-grained control that scales to secure your expanding universe of privileges, while creating a frictionless user experience.

ABOUT BEYONDTRUST

BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering organizations to secure and manage their entire universe of privileges. Our integrated products and platform offer the industry's most advanced PAM solution, enabling organizations to quickly shrink their attack surface across traditional, cloud and hybrid environments.

The BeyondTrust Universal Privilege Management approach secures and protects privileges across passwords, endpoints, and access, giving organizations the visibility and control they need to reduce risk, achieve compliance, and boost operational performance. We are trusted by 20,000 customers, including 70 percent of the Fortune 500, and a global partner network. Learn more at

beyondtrust.com