BeyondTrust

MICROSOFT VULNERABILITIES REPORT 2019

An Analysis of Microsoft Security Updates in 2018

TABLE OF CONTENTS

Introduction

The Microsoft Vulnerabilities Report 2019 analyzes the data from security bulletins issued by Microsoft throughout 2018. On the second Tuesday of every month, commonly referred to as "Patch Tuesday," Microsoft releases fixes for any vulnerabilities affecting Microsoft products. This report compiles these releases into a year-long overview, providing a more holistic view of whether vulnerabilities are increasing, and how many Microsoft vulnerabilities could be mitigated if admin rights were secured across organizations.

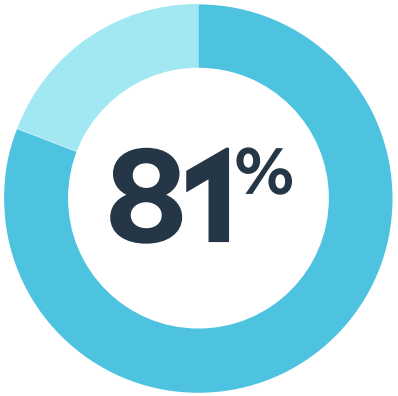
As the 2019 Microsoft Vulnerabilities report is the sixth annual edition, it includes a trend comparison based on several years of data. This analysis provides a better understanding of how vulnerabilities are growing, and in which specific products.

Microsoft vulnerabilities continued to rise in 2018, with a total of 700 vulnerabilities discovered.

700

VULNERABILITIES DISCOVERED

And while there are 46 less Critical Vulnerabilities than in last year's report, the findings indicate that the removal of admin rights would mitigate a higher percentage of Critical Vulnerabilities this year.



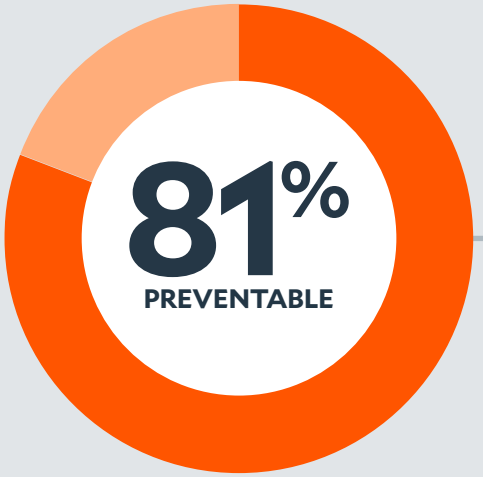
Of the **189 Critical Vulnerabilities discovered, 154 (81%) could have been prevented** if administrator rights had been secured.

> **"Least privileged access continues to be the way forward - we know with certainty that the removal of admin rights is one of the leading mitigating factors in keeping our networks and systems safe in the face of accelerating vulnerability disclosures."**
>
> ***— Kenneth Holley, Founder & CEO at Information Systems Integration***

DATA HIGHLIGHTS

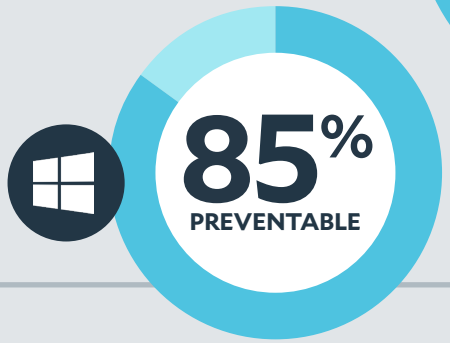
Overall number of reported vulnerabilities over 6 years. (2013-2018)

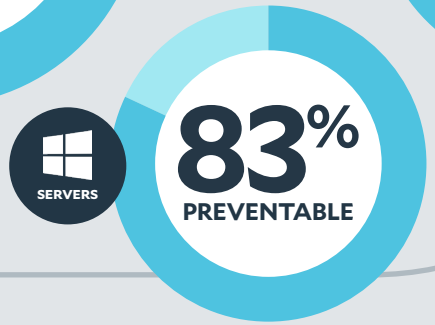
Critical vulnerabilities reported by Microsoft over 6 years. (2013-2018)



Of the **189 critical vulnerabilities discovered, 154 could have been prevented** if administrator rights had been removed.

Percentage of **critical vulnerabilities in Internet Explorer, Microsoft Office, Windows 7, 8.1, and 10, and Windows servers** that would have been mitigated by removing admin rights.



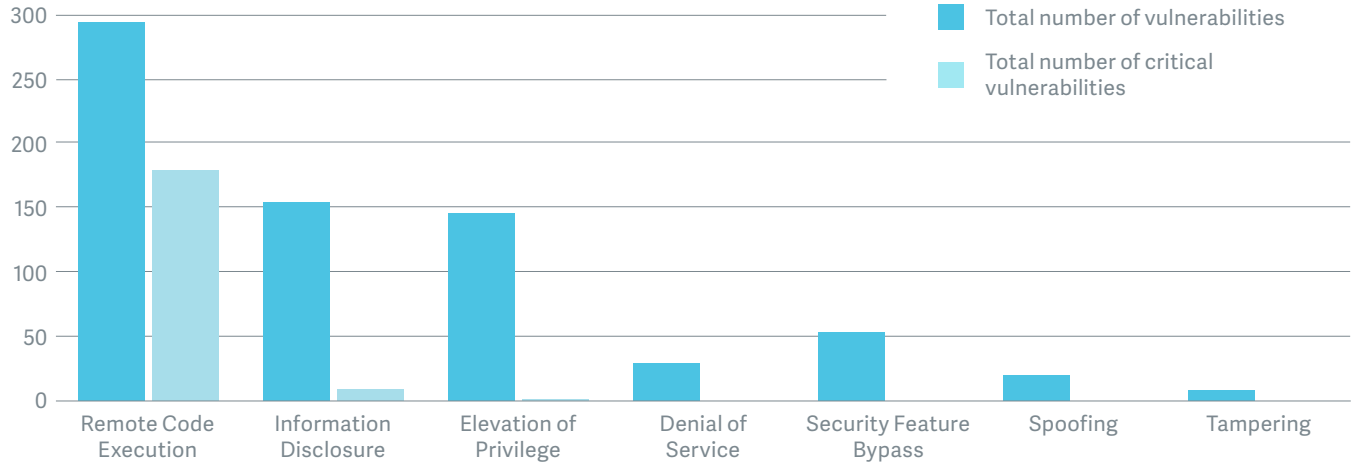


How Microsoft Groups Vulnerabilities

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

Similar to previous reports, Remote Code Execution (RCE) accounts for the largest proportion of total Microsoft vulnerabilities throughout 2018. Of the 292 RCE vulnerabilities, 178 were considered Critical. The removal of admin rights from Windows endpoints would have mitigated 86% of these Critical vulnerabilities. Over six years, RCE vulnerabilities are notably higher than they were in 2013, experiencing a 54% rise.

Breakdown of Microsoft Vulnerability Categories in 2018



	2013	2014	2015	2016	2017	2018
Remote Code Execution	190	257	303	269	301	292
Elevation of Privilege	99	39	108	114	90	145
Security Feature Bypass	4	16	35	26	41	53
Tampering	1	1	1	0	1	8
Information Disclosure	20	17	56	102	193	153
Denial of Service	19	13	13	0	43	29
Spoofing	1	2	9	12	16	20

Vulnerability Categories (2013-2018)

PRODUCT VIEW

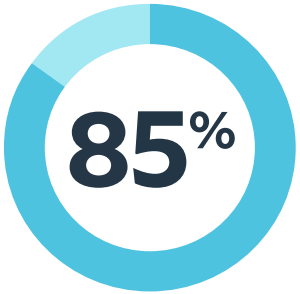
Windows Vulnerabilities

In 2018, 499 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 Microsoft has still reported vulnerabilities. While the overall number decreased from the prior year, the six year trend (2013-2018) shows almost twice the number reported over that time frame.

Of all the Windows vulnerabilities discovered in 2018, 169 of these were considered "critical".

Removing admin rights could have mitigated 85% of these critical vulnerabilities.

499
VULNERABILITIES DISCOVERED

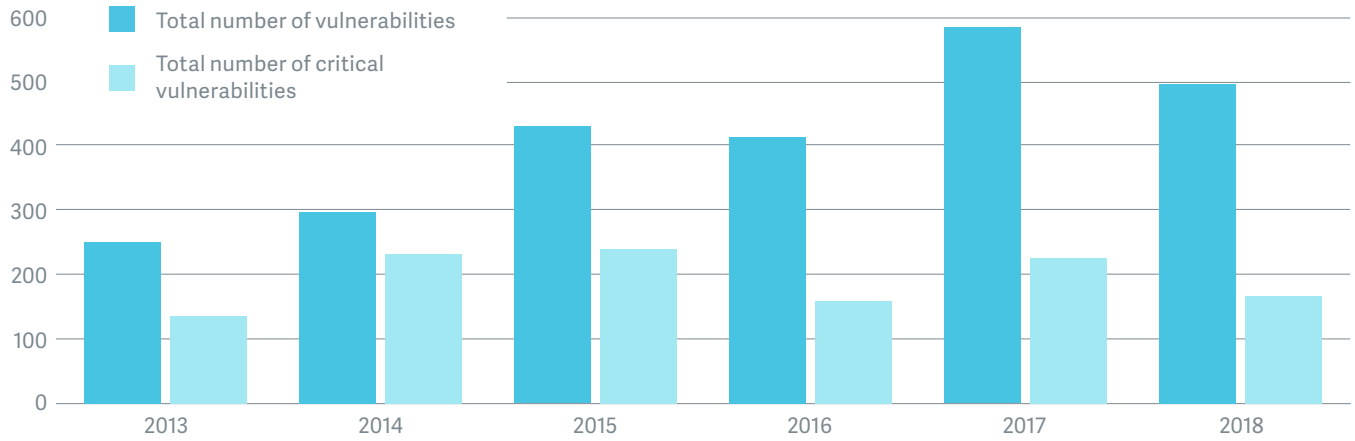


MITIGATED BY REMOVING ADMIN RIGHTS

INCREASE IN VULNERABILITIES SINCE 2013

169
CRITICAL VULNERABILITIES DISCOVERED

Microsoft Windows Vulnerabilities (2013-2018)



Internet Explorer & Edge Browser Vulnerabilities

Microsoft Internet Explorer remains a widely used browser, but since January 2016 Microsoft only supports and patches the most current version of Internet Explorer available for a supported operating system. Microsoft Internet Explorer (IE) 10 will reach end of support on January 31, 2020. From that point forward, IE 11 will be the only supported version of Internet Explorer on Windows Server 2012 and Windows Embedded 8 Standard.

Critical vulnerabilities in Microsoft Edge have increased six-fold since its inception two years ago. In the near future, Edge will have 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.

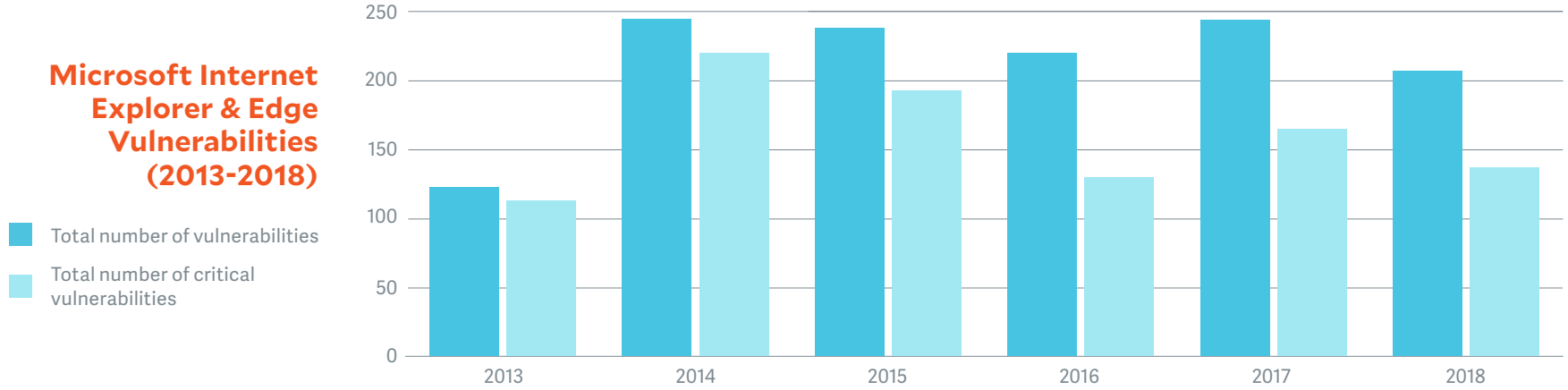
207
VULNERABILITIES DISCOVERED

92%
MITIGATED BY REMOVING ADMIN RIGHTS

68%
INCREASE IN VULNERABILITIES SINCE 2013*

137
CRITICAL VULNERABILITIES DISCOVERED

Microsoft Internet Explorer & Edge Vulnerabilities (2013-2018)



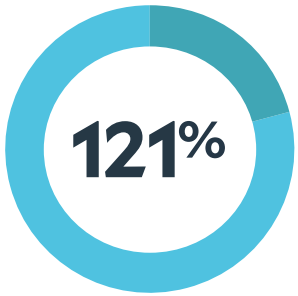
Microsoft Edge was released in 2017, so only 2 years of historical data are available.

Office Vulnerabilities

Vulnerabilities in Microsoft Office continue to rise year over year, and they hit a record high of 102 in 2018. Removing admin rights would mitigate 100% of critical vulnerabilities in all Microsoft Office products in 2018 (Excel, Word, PowerPoint, Visio, Publisher and others).

102
VULNERABILITIES DISCOVERED

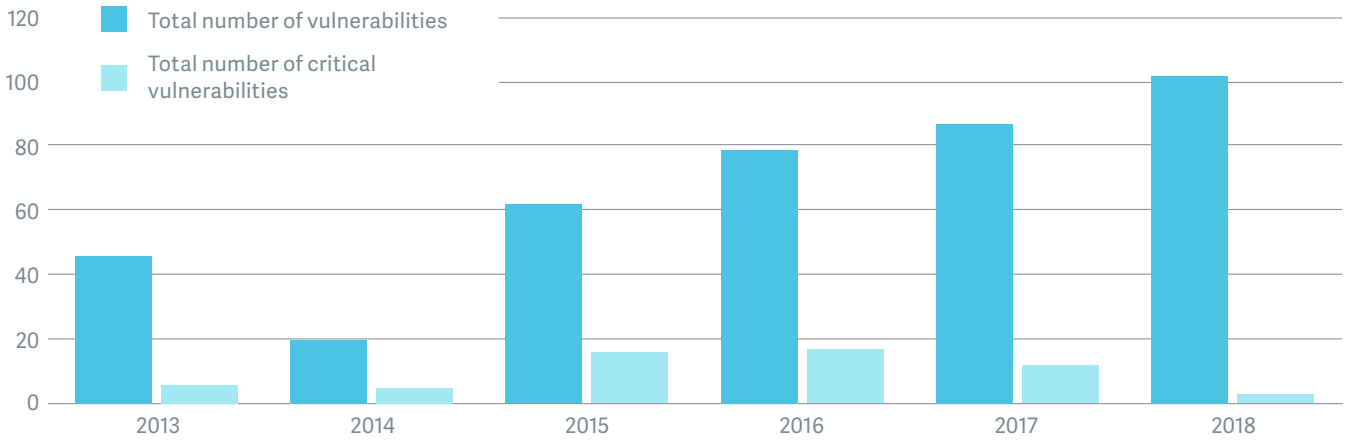
MITIGATED BY REMOVING ADMIN RIGHTS



INCREASE IN VULNERABILITIES SINCE 2013

3
CRITICAL VULNERABILITIES DISCOVERED

Microsoft Office Vulnerabilities (2013-2018)



Windows Server Vulnerabilities

A total of 449 vulnerabilities were reported in Microsoft Security Bulletins affecting Microsoft Windows Server in 2018. Of the 136 vulnerabilities with a critical rating, 83% could be mitigated by the removal of admin rights. In 2013, 252 vulnerabilities in Microsoft Windows Server were found - the number of vulnerabilities has almost doubled over the last six years.

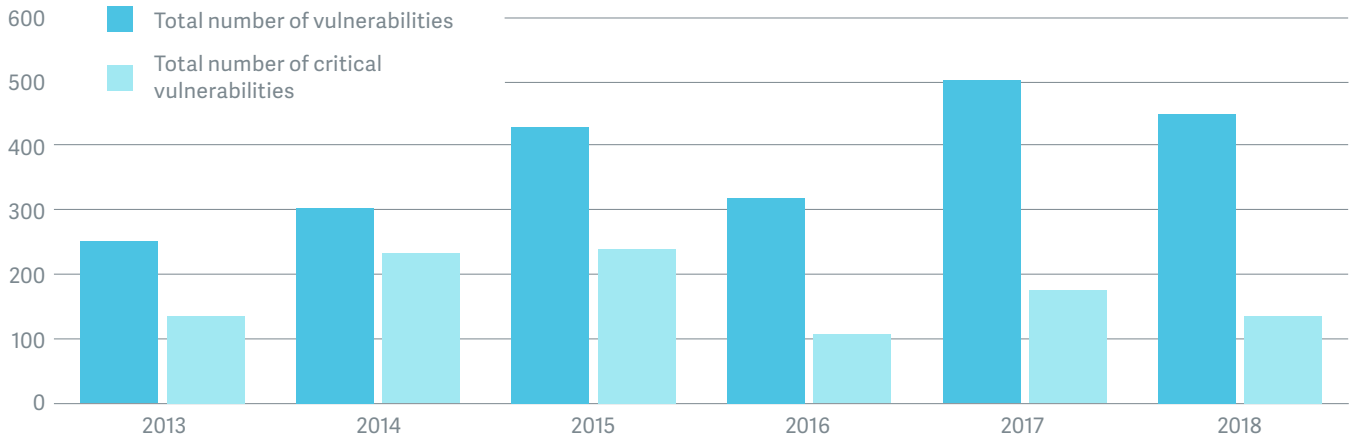
449
VULNERABILITIES DISCOVERED

83%
MITIGATED BY REMOVING ADMIN RIGHTS

78%
INCREASE IN VULNERABILITIES SINCE 2013

136
CRITICAL VULNERABILITIES DISCOVERED

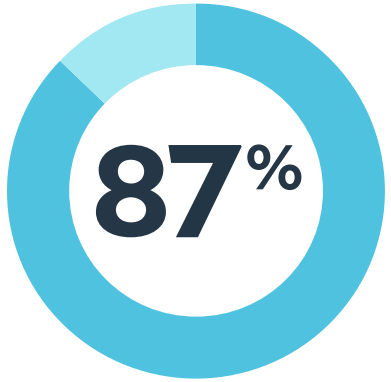
Windows Servers Vulnerabilities (2013-2018)



SECURITY IMPACT

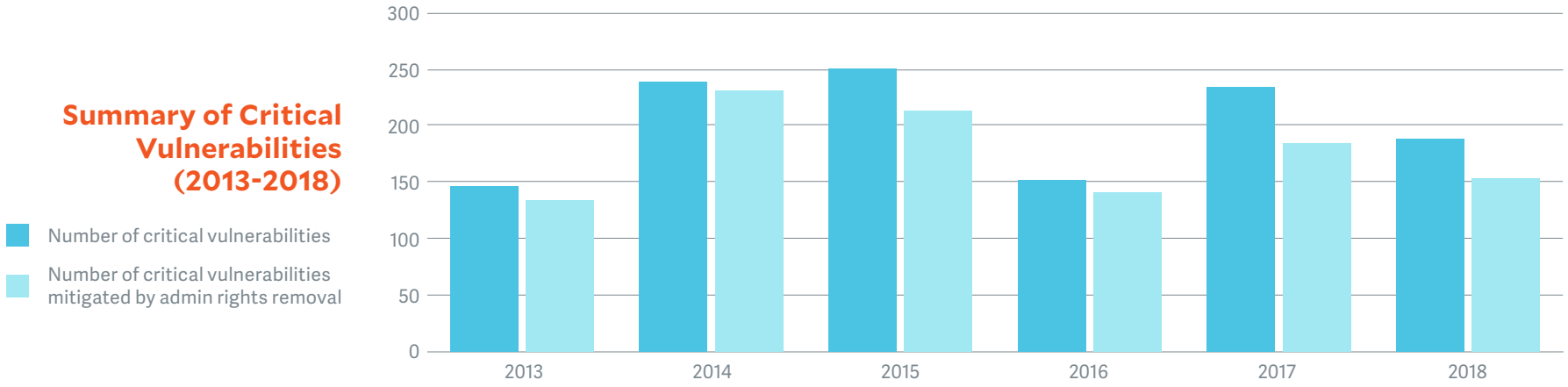
Microsoft Critical Vulnerabilities Continue To Impact Organizations

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 the vast majority of these vulnerabilities can be mitigated by the removal of local administrator rights. On average, over the last six years, **87% of all critical vulnerabilities** published by Microsoft **could have been mitigated by removing admin rights.**



OF ALL CRITICAL VULNERABILITIES COULD HAVE BEEN MITIGATED BY REMOVING ADMIN RIGHTS

Summary of Critical Vulnerabilities (2013-2018)



> **“This report highlights the issues with misconfiguration of users… it would seem that criminal hackers are gaining the upper hand. But, when we look at the context of these vulnerabilities, we can be more measured - and in fact more optimistic - in our response.”**
>
> ***— Jessica Barker, CEO of Cygenta***

Get Serious about Applying Least Privilege Principles

While eliminating admin rights can greatly improve security around Microsoft products and reduce the risks from their vulnerabilities, many IT leaders are concerned with how to balance access restrictions with maintaining a positive user experience.

Least privilege is the concept and practice of restricting access rights for users, accounts, and computing processes to only those resources absolutely required to perform routine, legitimate activities. Privilege itself refers to the authorization to bypass certain security restraints. Applied to people, least privilege, sometimes called the principle of least privilege (POLP), means enforcing the minimal level of user rights, or lowest clearance level, that allows the user to perform his/her role. However, least privilege also applies to processes, applications, systems, and devices (such as IoT), in that each should have only those permissions required to perform an authorized activity.

The tension between security and productivity is often the barrier that prevents organizations from removing local admin rights from all users. To address this challenge, modern endpoint privilege management solutions can be deployed to dynamically exert granular control over access to applications, tasks and scripts in a way that makes this balance seamless and the security invisible to the end user. These solutions elevate access as needed for applications — without elevating the user's actual privileges — to ensure that users are productive and protected.

Additionally, a vulnerability management solution closes any final gaps for the "worst of the worst" vulnerabilities, that can only mitigated by patch management.

MITIGATION

> **"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***

CISO Viewpoint

"The 2017 NotPetya attack (which caused at least $10 billion in world-wide damages) provides an excellent demonstration of how vulnerabilities in commonly used software have been weaponized. Because ransomware and disk wipers work so well, and because of static cybersecurity defences and digital weapons proliferation, we can expect to see more critical patches will be issued in the future.

> **"If routinely installing critical patches is the digital equivalent of washing your hands after using the toilet, then we collectively have terrible cyber hygiene."**

Did you know the patch to neutralize NotPetya had been released by Microsoft 90 days prior? If routinely installing critical patches is the digital equivalent of washing your hands after using the toilet, then we collectively have terrible cyber hygiene. The best way I know to improve your digital hand washing is to adopt the "Top 4" from the Australian Signals Directorate (ASD). These four mitigations have been selected and prioritized specifically to counter the delivery and execution of malicious code, including those vulnerabilities that can be exploited without warnings or prompts. These practices can apply to any company concerned about preventing data breaches as the ASD has many similarities with the mandates for GDPR, NIST, and PCI.

The four, in order, are: Application whitelisting; Patch applications; Restrict administrative privileges; and Patch operating systems. ASD says properly implementing the Top 4 will mitigate over 85% of the collective adversary's targeted malicious code techniques.

Here's an example: In a prior CISO role, my team removed local admin rights for our entire company of about 1,000 desktop and laptop computers. Lots of people told us it couldn't be done. But, in the end our people were even more productive without local admin rights."

KIP BOYLE
CEO, Cyber Risk Opportunities

linkedin.com/in/kipboyle

@KipBoyle

cyberriskopportunities.com

firedoesntinnovate.com

Academic Viewpoint

"The data does not lie! It has been clearly demonstrated that despite the many advances in cybersecurity techniques and technology the number of vulnerabilities continues to drastically increase year after year - with no end in sight.

This increase can be attributed to the fact thatno matter how much attention is given to new advances in technology, the amount of attention given to who can access what data is often lacking. An organization's critical assets face threats that extend beyond the realm of technology. Its processes and employees can expose sensitive data in ways that cannot be mitigated with technical controls alone.

While organizations take actions to control access to its highly sensitive information with strict access controls, other types of data are often left "wide open." This means that anyone who uses seemingly legitimate credentials to access the network can access most of the organization's data.

I have emphasized many times that if you want to reduce organizational security risks, you must control access, especially to privileged accounts. The simple fact is that if you're going to prevent bad actors from getting in and insiders from abusing access privileges, you must have expert management of your privileged accounts.

While there is no silver bullet for achieving full-proof cybersecurity, organizations can dramatically reduce the impact of an attack by prioritizing privileged access. Organizations must choose the right access control model based on the types of data they process, how sensitive that data is, and operational requirements. With a good privilege access management model and processes, these organizations can enforce least privilege policies. This will empower them to reduce the threat of security attacks & data breaches.

"While there is no silver bullet for achieving full-proof cybersecurity, organizations can dramatically reduce the impact of an attack by prioritizing privileged access."

Privileged access management acts as a secure repository, or vault, that protects an organization's data and networks. By adopting privileged user management, an organization can ensure that users only access the data required to do their job. IT teams will be able to establish parameters that will prevent users from accessing systems and information that they should not.

As a university professor, I tell my students that security is really very simple. Control access to control the threat! If bad guys cannot get into an environment in the first place, they can do no harm."

PROFESSOR DEREK A. SMITH

Speaker, Author & University Professor, President of the Intercessor's Investigative & Training Group

linkedin.com/in/dsmith8952

@DerekASmith1

facebook.com/derekasmith53

theintercessorgroup.com

CEO Viewpoint

"It is often easy to be pessimistic when seeing that the number of vulnerabilities found per year has grown at an alarming rate. With a 110% rise in the last six years, it would seem that criminal hackers are gaining the upper hand. But, when we look at the context of these vulnerabilities, we can be more measured - and in fact more optimistic - in our response. More vulnerabilities are being discovered partly because more and more software is being developed every year. But more vulnerabilities are also being discovered because we as an industry are getting smarter and better and faster at finding and disclosing them, with more people than ever are looking for vulnerabilities compared to six years ago. We have also seen more organizations hiring penetration testers and setting up bug bounty programs.

If we look at the history of vulnerabilities we see that the same classes of vulnerabilities have constantly appeared at the top of the OWASP (Open Web Application Security Project) Top 10 and it is shocking that certain classes, such as SQL Injection and XSS, are still such a big problem today. This report highlights the issues with misconfiguration of user privileges and it would be easy to demand that systems administrators do not offer administrative rights to all users and to argue that they are lax when applying patches to systems. But it is easy to pick fault with people when, in fact, surrounding factors are sometimes pushing people to behave in certain ways.

"The Microsoft Vulnerabilities Report 2019 supports the importance of least privilege models, proving that reducing the number of admin users is a necessary step in the foundation of your security strategy."

The Microsoft Vulnerabilities Report 2019 supports the importance of least privilege models, proving that reducing the number of admin users is a necessary step in the foundation of your security strategy. Reviewing and verifying access lists is an important, and often overlooked, part of that process. Likewise, whitelisting applications is an effective mitigation, but people and processes need to be in place to manage whitelisting to prevent it from becoming perceived as a business-blocker."

DR. JESSICA BARKER
Co-CEO of Cygenta & Chair of ClubCISO

@drjessicabarker

@CygentaHQ

cygenta.co.uk

Service Provider Viewpoint

"During the security assessments we have conducted in the past few years, we've noticed that one of the most common issues observed is the extensive usage of privileged accounts by users who do not need them for daily work. Sometimes, this practice makes users' work easier, but as the Microsoft Vulnerabilities Report demonstrates, it also opens many dangerous attack vectors and is one of the main reasons why ransomware has been spreading so successfully.

The running of malicious code by a user with administrative privileges may allow the attacker to perform a lot of different activities; for example, it allows to access the memory of system processes like LSASS to extract users' credentials, including password hashes and other sensitive data. Once hashes are obtained, the attacker may use them to perform Pass-The-Hash attacks to gain access to other machines in the network. Another scenario to consider is whether privileged users may be able to turn off endpoint protection mechanisms like antivirus solutions or hide malicious activities, which prolong the time of discovering them. Privileged Access Management solutions that include securing, managing, and controlling endpoints and passwords reduce these types of risks.

A successful cyber attack may result in an extensive financial loss for the company and disclosure of confidential information and know-how. The attack may also cause disruption of services provided by the company, like online services, production lines or by leading to physical damage of devices. That's why it's also advisable to perform penetration tests as they are one of the most efficient ways to identify technical vulnerabilities in the company's IT infrastructure before the attack occurs. The main goal of each test is to find as many vulnerabilities as possible that could make the work of a potential hacker much easier and put the organization at immense risk. After a penetration test is performed by companies specializing in security, like CQURE, a report is prepared with a detailed description of all findings with recommendations on resolving them, making it much easier for the customer to implement crucial mitigations.

"During the security assessments we have conducted in the past few years, we've noticed that one of the most common issues observed is the extensive usage of privileged accounts by users who do not need them for daily work."

PAULA JANUSZKIEWICZ
Cybersecurity Expert & CEO of CQURE

linkedin.com/in/paulajanuszkiewicz

@paulacqure

cqureacademy.com

ABOUT THIS REPORT

The BeyondTrust Analysis - 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 are stated by Microsoft in 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 2018, 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 10)

About BeyondTrust

BeyondTrust is the worldwide leader in Privileged Access Management, offering the most seamless approach to preventing data breaches related to stolen credentials, misused privileges, and compromised remote access. Our extensible platform empowers organizations to easily scale privilege security as threats evolve across endpoint, server, cloud, DevOps, and network device environments. BeyondTrust gives organizations the visibility and control they need to reduce risk, achieve compliance objectives, and boost operational performance. We are trusted by 20,000 customers, including half of the Fortune 100, and a global partner network.

About Endpoint Privilege Management

BeyondTrust's Endpoint Privilege Management solutions give you the power to enforce least privilege and eliminate local admin rights. Remove excessive end user privileges and control applications on Windows, Mac, Unix, Linux, and network devices - all without hindering end-user productivity.

About Vulnerability Management

BeyondTrust's Vulnerability Management solutions reduce risk with cross-platform vulnerability assessment and remediation, including built-in configuration compliance, patch management and compliance reporting.

beyondtrust.com