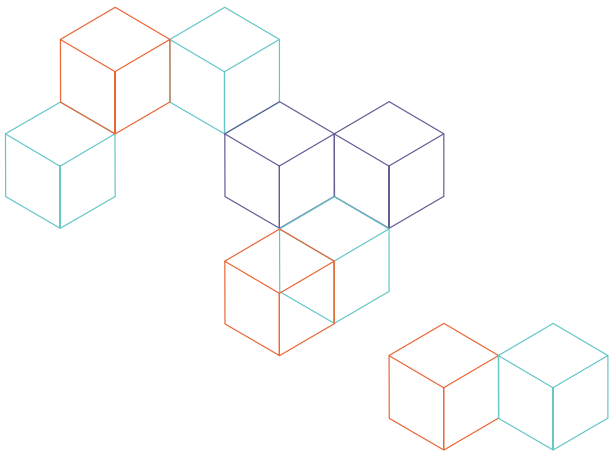
Avecto

MICROSOFT *VULNERABILITIES* REPORT 2017

SECURITY FUNDAMENTALS

Avecto



Avecto

Introduction

Compiled by Avecto, this report analyses the data issued by Microsoft via the Security Update Guide throughout 2017. The Security Update Guide focuses on security vulnerabilities affecting all Microsoft products and services. This report compiles the available information into a year-long overview, allowing us to deduce whether vulnerabilities are increasing, and, more importantly, how many Microsoft vulnerabilities could be mitigated if admin rights were removed from organizations.

2017 is particularly special, as it marks the fifth year of the Microsoft Vulnerabilities Report, so we'll review the trends we've seen during that time. The increase in Microsoft vulnerabilities for 2017 makes a bigger leap from last year than we've seen before. A total of 685 vulnerabilities were found, adding some 234 onto last year's total, and more than doubling the 325 found in 2013.

As such, we've seen a 54% increase in Critical Microsoft vulnerabilities since 2016.

Time and again in these reports we see how removing admin rights is the most effective step to take in mitigating these vulnerabilities, and this year is no different. Removing admin rights would mitigate the risk of 80% of all Critical Microsoft vulnerabilities in 2017.

> "The common misconception is that a user with local admin rights can do little harm and that administrative actions taken at the endpoint are isolated to the endpoint itself. Neither assertion is true."
>
> Gartner, Inc., "Reduce Access to Windows Local Administrator with Endpoint Privilege Management,"
>
> **Lori Robinson, October 20, 2017**

Methodology

Security vulnerability and update information issued by Microsoft contains a summary with general information regarding that vulnerability. For this report, a vulnerability is classed as one that could be mitigated by removing admin rights if the sentence "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" or "If the current user is logged on with administrative user rights, an attacker could take control of an affected system" is found within the summary of that specific vulnerability.

Key findings

The 2017 report highlights the following key findings:

- Removing admin rights would mitigate 80% of all Critical Microsoft vulnerabilities in 2017.
- The number of reported vulnerabilities has risen 111% over five years (2013-2017).
- There has been a 54% increase in Critical Microsoft vulnerabilities since 2016 and 60% in five years (2013-2017).
- 95% of Critical vulnerabilities in Microsoft browsers can be mitigated by removing administrator rights.
- There has been an 89% increase in Microsoft Office vulnerabilities in the past five years.
- Almost two thirds of all Critical vulnerabilities in Microsoft Office products are mitigated by removing admin rights.
- Despite being widely regarded as the most secure Windows OS ever, Windows 10 vulnerabilities rose by 64% in 2017.
- Removing admin rights would mitigate almost 80% of Critical vulnerabilities in Windows 10 in 2017.
- Critical vulnerabilities in Microsoft Browsers are up 46% since 2013.
- 88% of all Critical vulnerabilities reported by Microsoft over the last five years would have been mitigated by removing admin rights.

Avecto

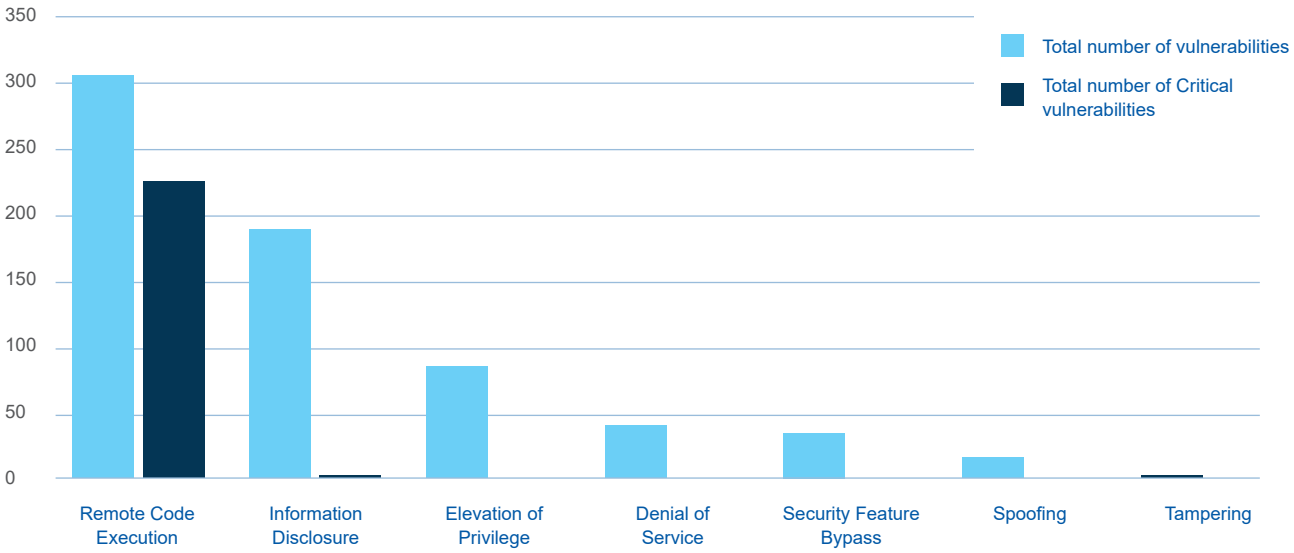
Vulnerability categories

Each vulnerability is categorized by impact for each specific product it affects. These categories consist of: Remote Code Execution, Elevation of Privilege, Information Disclosure, Denial of Service, Security Feature Bypass, Spoofing and Tampering.

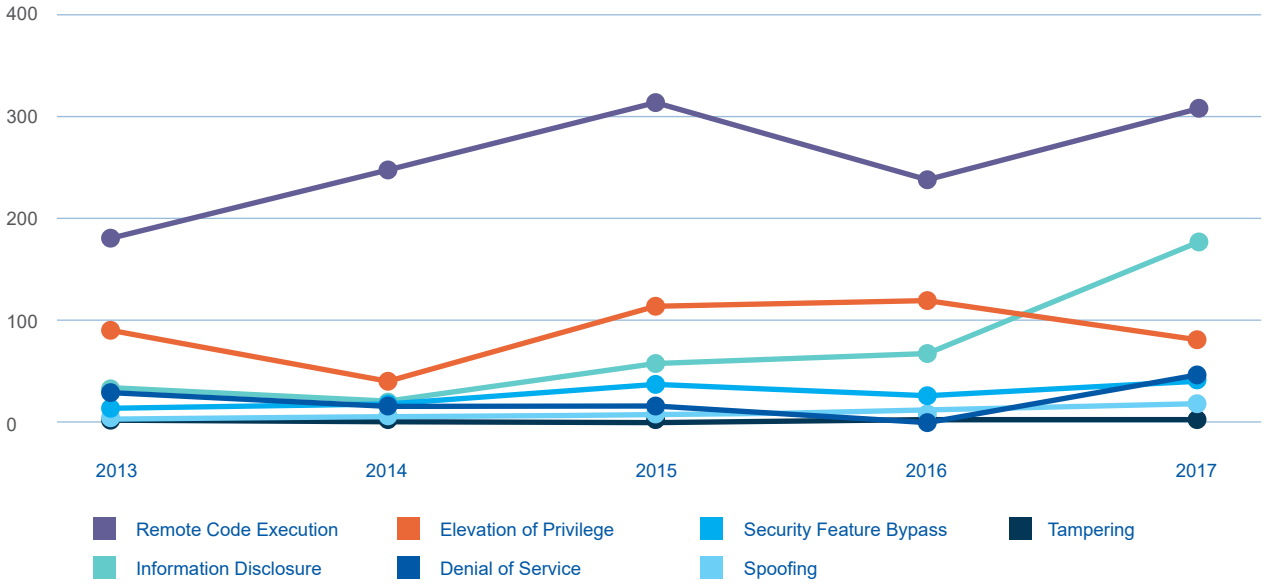
As per previous reports, Remote Code Execution (RCE) account for the largest proportion of total Microsoft vulnerabilities throughout 2017. Of the 301 RCE vulnerabilities, 231 were considered Critical. Of these Critical vulnerabilities, the removal of admin rights would have mitigated 80%.

From a 5 year perspective, RCE vulnerabilities are notably higher than they were in 2013, experiencing a 58% rise.

Breakdown of Microsoft Vulnerability categories in 2017



5 year overview (2013 - 2017)



Avecto

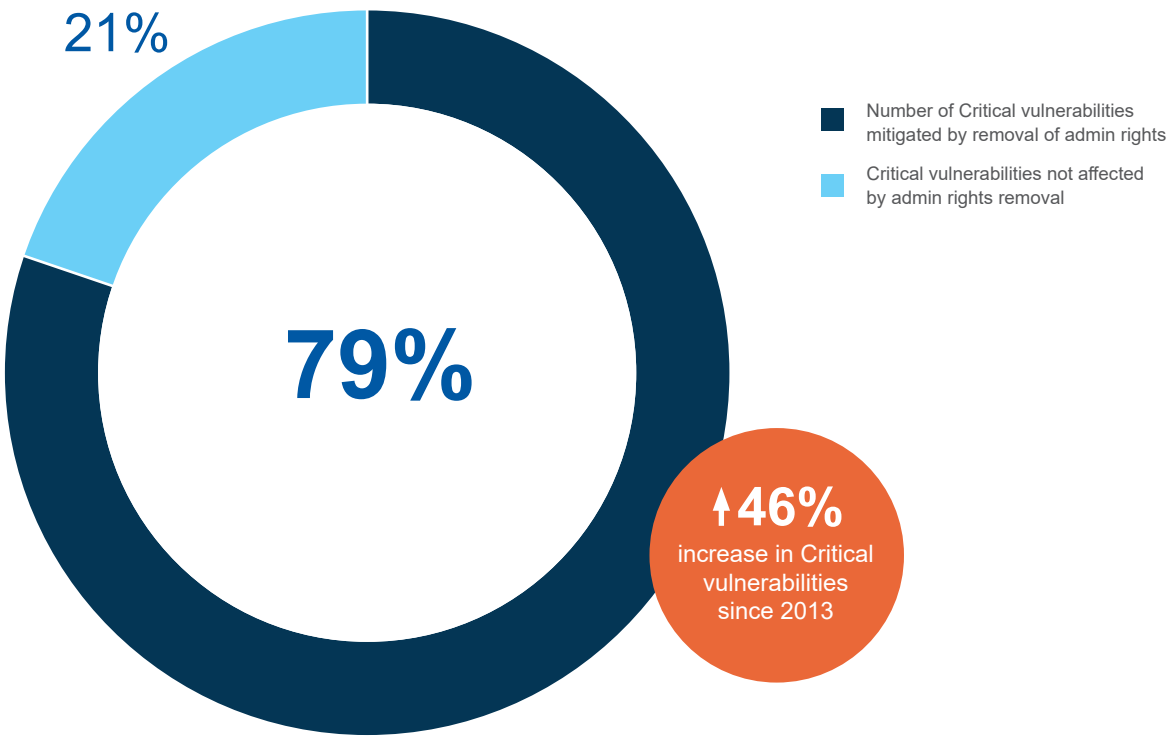
Microsoft Windows vulnerabilities

In 2017, 587 vulnerabilities were reported across Windows Vista, Windows 7, Windows RT, Windows 8/8.1 and Windows 10 operating systems. **This is a record high, coming in 232 vulnerabilities more than last year's report, and marking a 132% increase on the numbers from 5 years ago.**

Critical vulnerabilities in Microsoft browsers are up by 46% since 2013.

79% of Critical vulnerabilities affecting Microsoft Windows in 2017 could be mitigated by the removal of admin rights.

Critical Windows vulnerabilities mitigated by removal of admin rights in 2017



"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 and CEO of Secure Anchor Consulting

Avecto

Microsoft Edge

Of the 140 Critical vulnerabilities found in Microsoft's Edge browser in 2017, 134 could have been mitigated if admin rights had been removed. Critical vulnerabilities in Microsoft Edge have increased seven-fold since its inception two years ago.

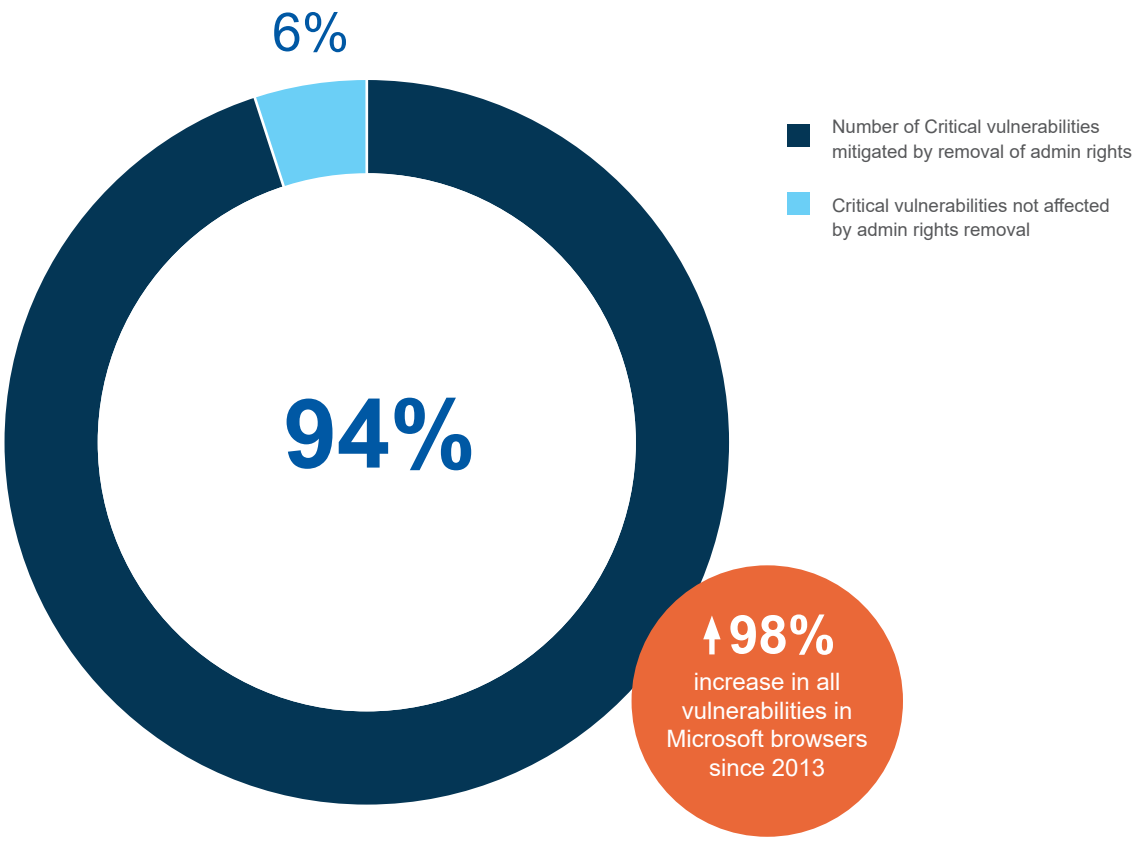
The removal of admin rights would mitigate 96% of Critical vulnerabilities found in Microsoft's Edge browser in 2017.

Internet Explorer

Of the 48 Critical vulnerabilities discovered in Internet Explorer (IE) versions 8-11 in 2017, 45 would have been mitigated through removing admin rights.

There has been a 98% increase in all vulnerabilities in Microsoft browsers since 2013.

Internet Explorer vulnerabilities mitigated by removal of admin rights in 2017

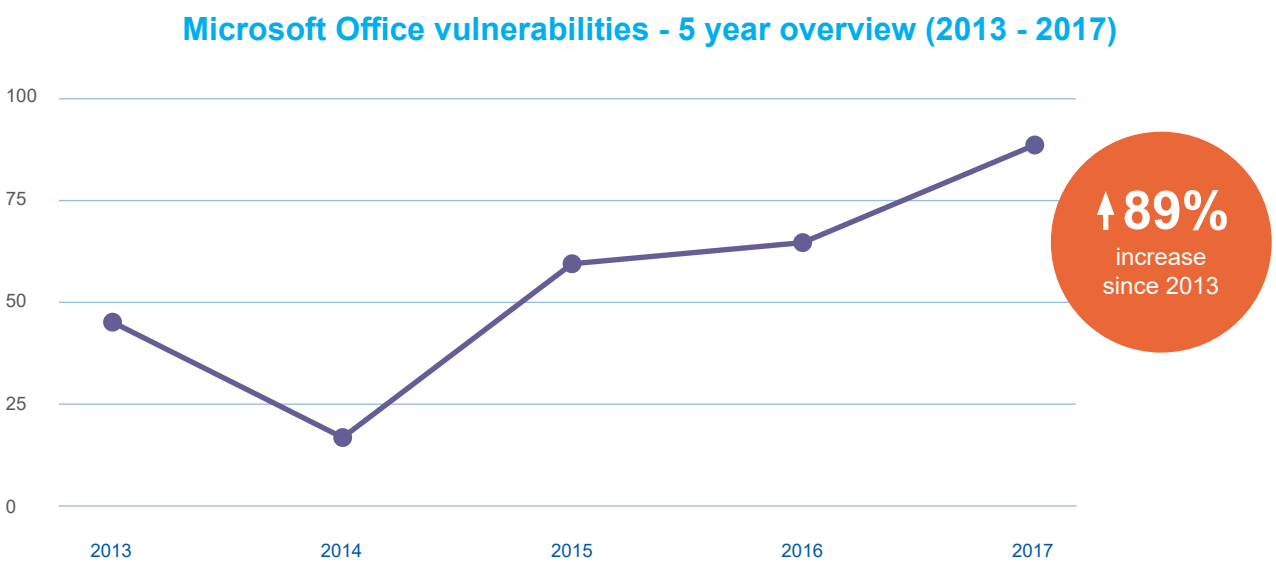


Avecto

Microsoft Office

Vulnerabilities in Microsoft Office continues to see a year-on-year rise, as they hit a record high of 87 in 2017. Since 2013, Critical vulnerabilities have doubled, albeit from just 6 to 12.

Removing admin rights would mitigate 60% of Critical vulnerabilities in all Microsoft Office products (Excel, Word, PowerPoint, Visio, Publisher and others).



"Among several foundational aspects of Zero Trust is that of least privileged access - we know with certainty that 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. I believe that 2017 will come to be known as a watershed year for security, a wake-up call for organizations, and a realization that a mature security posture isn't a destination, rather an ongoing journey."

Kenneth Holley, Founder & CEO at Information Systems Integration

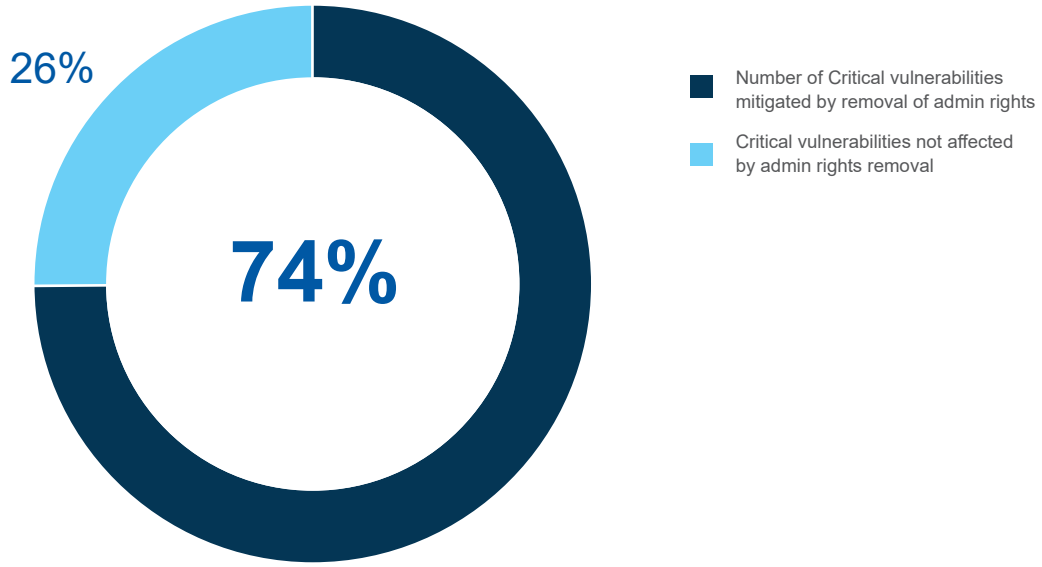
Avecto

Windows Server vulnerabilities

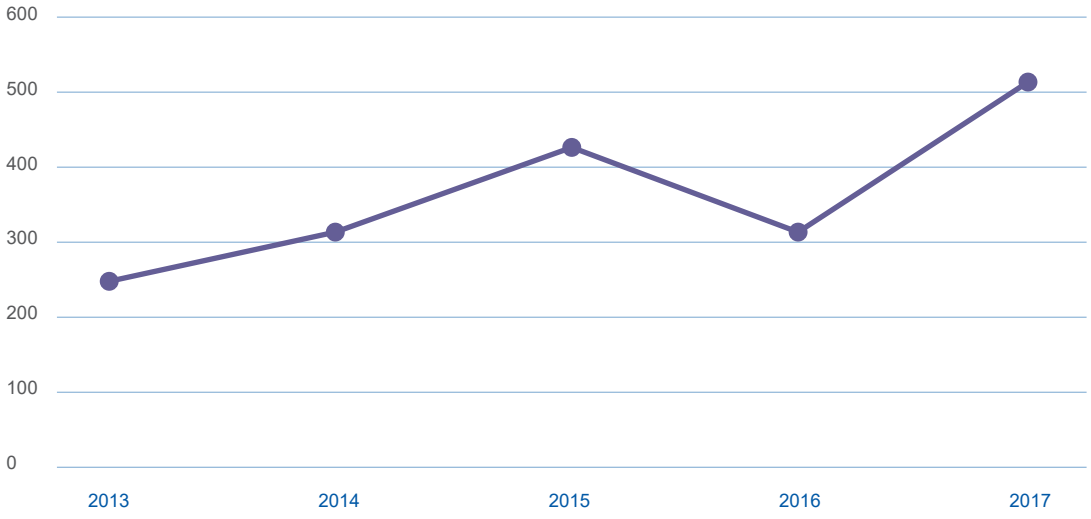
A total of 501 vulnerabilities were reported in Microsoft Security Bulletins affecting Microsoft Windows Server in 2017. Of the 176 vulnerabilities with a Critical rating, 74% could be mitigated by the removal of admin rights.

In 2013, 252 vulnerabilities in Microsoft Windows Server were found, meaning that the number of vulnerabilities has doubled over the last 5 years. The largest rise during this period occurred this year, with a 65% increase over the 303 vulnerabilities found in our 2016 report.

Windows Server Critical vulnerabilities mitigated by removal of admin rights in 2017



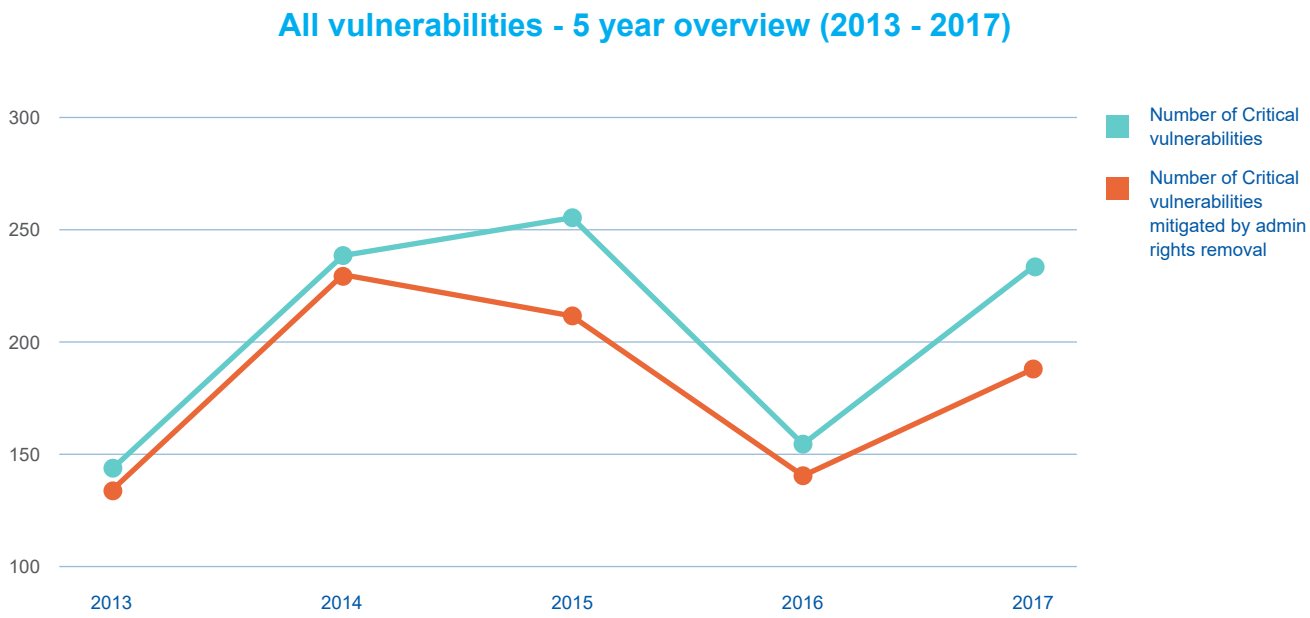
Windows Server vulnerabilities - 5 year overview (2013 - 2017)



Avecto

Conclusion

We can see that, since 2013, Critical vulnerabilities have grown and should be of some concern to organizations. However, our report continues to prove that the majority of these Critical vulnerabilities could be mitigated by the removal of local administrator rights. In fact, more than 88% of all Critical vulnerabilities reported by Microsoft over the last five years would have been mitigated by removing admin rights.



So why are organizations still not taking note?

According to Gartner, "Reducing access to local administrator rights is one of the best things you can do to improve Windows security. However, balancing access restrictions with user experience is a challenge that many businesses fail to get right." Gartner, Inc., "Reduce Access to Windows Local Administrator with Endpoint Privilege Management," Lori Robinson, October 20, 2017.

It is this balance between security and usability that is often the barrier for organizations removing local admin rights from all users. Endpoint privilege management software is deployed to provide granular control over access to applications, tasks and scripts to ensure that users are productive but permissions are never elevated.

Jake Williams, President of Rendition InfoSec, recommends asking yourself "Does this user have access to particularly sensitive information (perhaps with regulatory compliance requirements)? Is the machine being used exposed directly to the Internet (e.g. mail or web server)? Is the machine regularly used to surf the Internet or open email from outside the organization? If the answer to any of these questions is yes, prioritize patching this machine and removing administrative rights from the users who log in there.

It's hard to stress the last point enough - in my incident response work, I find that web browsing and email attachments (PDF, Microsoft Office, etc.) are the ways that vulnerabilities are most often remotely exploited to gain access into an organization. Removing admin rights won't prevent a vulnerability from being exploited, but it will limit what an attacker can do after they gain initial access. If the attacker doesn't have local admin, they're likely to make a lot of noise trying to get it, and this creates opportunities for detection, putting you back on the winning team."

Avecto

Expert commentary

Dr. Eric Cole, Founder and CEO, Secure Anchor Consulting

“One hundred percent security cannot be guaranteed in the cyber world. No matter how many safeguards you put in place, there will always be some risk. This is based on the simple premise that if you are 100% secure, there is no functionality. As soon as you add functionality, it will decrease the overall security. Therefore the simple analysis to always perform when adding functionality is whether it is worth the overall security exposures.

The problem is that most companies only look at the benefit of a new functionality but never ask the follow-up questions:

What is the security risk associated with this functionality?

Are there other more secure alternatives?

This gap in performing proper analysis is never more evident than with administrator access. A user or business unit complains that they need administrator access and, without verifying or validating the request, they are given the access without the proper analysis.

If you want to be secure, users cannot be logged in as an administrator. If you are like many companies that I work with, the initial response is that they need or require that access – those are very strong words. A premise that should drive all security decisions is to let data drive decisions, not emotions – do the math. What benefit do you gain by providing them with administrator access versus the potential increase in exposure or damage to the company by allowing the access? If you do proper analysis, you will find what Avecto discovered: that taking away administrator access can mitigate 80% of all Critical vulnerabilities and 95% of Critical vulnerabilities in browsers.”

Bio

Dr. Eric Cole is a renowned security expert with over two decades of in-the-trenches experience in IT and network security. He is the author of several books and textbooks, including Advanced Persistent Threat, Hackers Beware, Hiding in Plain Sight, Network Security Bible 2nd Edition, and Insider Threat, and has presented at many major conferences. He also served as a member of the Commission on Cyber Security for the 44th President, Barack Obama, and sits on several executive advisory boards.

@DrEricCole

https://www.linkedin.com/in/ericcole1/

secure-anchor.com

Avecto

Expert commentary

Jake Williams, President of Rendition Infosec

“Removing admin rights from your users is one of the most important things you can do to mitigate vulnerabilities. Some organizations believe that user account control (UAC) will protect them, but attackers know of many methods to silently bypass UAC pop-ups. Even Microsoft says that UAC is not a security control. By removing administrative rights from your users, you ensure that the attacker cannot take full control of a machine even if a vulnerability is exploited.

Ideally all machines would be patched immediately and users wouldn’t have local admin on their machines. But we live in the real world and often organizations are dealing with years of technical debt and poor architecture decisions. We often have to prioritize our remediation actions. When prioritizing patching and removing admin rights, consider a few relevant points:

Does this user have access to particularly sensitive information (perhaps with regulatory compliance requirements)? Is the machine being used exposed directly to the Internet (e.g. mail or web server)? Is the machine regularly used to surf the Internet or open email from outside the organization? If the answer to any of these questions is yes, prioritize patching this machine and removing administrative rights from the users who log in there.

It’s hard to stress the last point enough - in my incident response work, I find that web browsing and email attachments (PDF, Microsoft Office, etc.) are the ways that vulnerabilities are most often remotely exploited to gain access into an organization. Removing admin rights won’t prevent a vulnerability from being exploited, but it will limit what an attacker can do after they gain initial access. If the attacker doesn’t have local admin, they’re likely to make a lot of noise trying to get it, and this creates opportunities for detection, putting you back on the winning team.”

Bio

Infosec professional. Breaker of poorly written software. Incident responder. Digital defender. Business bilingual. I treat infosec like the Hippocratic Oath: First do no harm. I help businesses create secure environments that actually function by addressing realistic risk. I help penetration test organizations so they can find the weak spots before an attacker does. When an attacker does find a weak spot first, I work with them to remove the attacker, assess the damage, and remediate the vulnerabilities that allowed the attacker access in the first place.

@MalwareJake

https://www.linkedin.com/in/jacob-williams-77938a16/

renditioninfosec.com

Avecto

Expert commentary

Kenneth Holley, Founder & CEO at Information Systems Integration

“There’s no mistaking the rise in Critical vulnerabilities over the past 5 years, a trend which cannot be ignored. While a proactive patching protocol is immensely important, it’s only a portion of a well-rounded cybersecurity posture. If not already implemented, organizations of all sizes should move with determined swiftness to implement the Zero Trust model of security, guided by the NIST Cybersecurity Framework.

Among several foundational aspects of Zero Trust is that of least privileged access - 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. I believe that 2017 will come to be known as a watershed year for security, a wake-up call for organizations, and a realization that a mature security posture isn’t a destination, rather an ongoing journey.”

Bio

With a particular focus on infrastructure security and data analytics, Kenneth has assisted many clients, including foreign sovereigns, to ensure brand and profile security, as well as building engaged communities within the social media realm. In addition to being a fervent technology evangelist and maintaining many industry-specific certifications, Kenneth is an established subject matter expert on digital technology security and new media, and he is a frequent contributor to technology-related publications. Mr. Holley proudly served in the United States Navy for six years and resides with his wife and their three children.

@KennethHolley

https://www.linkedin.com/in/kennethholley/

silentquadrant.com

Avecto

Expert commentary

Sami Laiho, Microsoft MVP and Ethical Hacker

“Looking at the Microsoft Vulnerabilities Report for 2017 a few things seem to stand out. The number of vulnerabilities and Critical vulnerabilities both increased by more than 50% from the previous year. In the long run the increase is even bigger so it’s a trend, not just a bad year. At the same time Microsoft found more than one million new malware samples per day.

If you look at the amount of vulnerabilities that could possibly be exploited it’s easy to understand that proactive security is way more important than reactive security. Windows has two rules for security to even be achievable:

1. **You need Full Disk Encryption (BitLocker etc) or great physical protection**

2. **You need to use the Principle of Least Privilege**

If you don’t have FDE it’s child’s play to get administrative access, and if you allow administrative rights to end-users they can disable FDE. For years, most security fronts have recommended least privilege as the most needed security feature out there. From my point of view, it still is - as it would have blocked 80% of vulnerabilities. For 2018 the most recommended feature by most is now whitelisting. Instead of trying to blacklist one million bad things a day, you list a few good ones every month. In real life, whitelisting is ineffective and very painful to manage unless you first reach the principle of least privilege. Organizations like NATO for example, require whitelisting from their own and their partners’ systems.

With security suites like Avecto Defendpoint I achieve what I need for both least privilege and whitelisting, on both Windows Enterprise and Professional versions. When you have this in place, you just need to add FDE that works like a glue for your security keeping your configuration intact and tamper free.”

Bio

Sami Laiho is one of the world’s leading professionals in the Windows OS and Security field. Sami has been working with and teaching OS troubleshooting, management, and security for more than 20 years. Sami’s session was evaluated as the best session in TechEd North America, Europe and Australia in 2014, the Nordic Infrastructure Conference in 2016 and 2017, and the Best External Speaker at Ignite 2017. Sami is also an author at PluralSight and the newly appointed conference chair at the TechMentor conference.

@SamiLaiho

https://www.linkedin.com/in/samilaiho/

samilaiho.com

Avecto

Expert commentary

Wendy Nather, Director of Advisory CISOs at Duo Security

“There are several possible explanations for the rise in vulnerabilities, and especially the increase in Critical vulnerabilities. Microsoft has been running a successful bug bounty program (created by Katie Moussouris) for years now, and that may well be pulling in the more important bug reports that would otherwise have been sold off to threat actors. As new classes of vulnerabilities are discovered, researchers tend to focus their efforts in those areas in a kind of “swarming” effect. Finally, whenever we see functionality being added to systems, the bugs will inevitably follow. Progress exacts a security tax.

What can organizations do to mitigate these vulnerabilities? Over and over again, we hear the same recommendations: keep up with patching, remove admin rights from regular users, and use whitelisting. People assume these things are hard to do, particularly in a legacy environment where both technology and user processes have solidified over years in response to business imperatives. But when the vast majority of Microsoft vulnerabilities can be mitigated by removing admin rights, there is really no alternative, particularly for budget-strapped enterprises. Patching is not a substitute for removing admin rights; nor is whitelisting. Cutting back on the scope of what actions can be performed with a user’s privileges, whether on purpose or by accident, is the most straightforward way to reduce security risk.”

Bio

Wendy Nather is Director of Advisory CISOs at Duo Security. She was previously the Research Director at the Retail ISAC, as well as Research Director of the Information Security Practice at independent analyst firm 451 Research. Wendy led IT security for the EMEA region of the investment banking division of Swiss Bank Corporation (now UBS), and served as CISO of the Texas Education Agency. She speaks regularly on topics ranging from threat intelligence to identity and access management, risk analysis, incident response, data security, and societal and privacy issues. Wendy is co-author of The Cloud Security Rules, and was listed as one of SC Magazine’s Women in IT Security “Power Players” in 2014.

@WendyNather

https://www.linkedin.com/in/wendynather/

duo.com

Avecto

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, 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 7 on Windows XP SP2.

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.

Certain vulnerabilities have occurred multiple times throughout 2017, usually affecting different software. In these cases, the vulnerability itself is only counted once, with all affected software types attributed to that one entry for the benefit of clarity and removal of duplication.

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 to certain software were also considered a vulnerability to the edition of Windows named as a combination.

  E.g. a vulnerability for Internet Explorer 11 on Windows 10 is taken as a vulnerability for Internet Explorer 11 and Windows 10.

About Avecto

For organizations seeking to prevent breaches without hindering productivity, Avecto combines best-in-class privilege management and application control software, making admin rights removal simple and scalable across desktops and servers to ensure compliance, security, and efficiency.

Since 2008, the company has enabled over 8 million users across the world's biggest brands and most highly-regulated industries to successfully work from the safety of standard user accounts while enjoying the flexibility of admin accounts.

About Defendpoint

Avecto Defendpoint is an endpoint privilege management tool, making admin rights removal simple in order to ensure compliance, security, and efficiency. It deploys in hours and leverages more than two dozen validation criteria to elevate applications securely and flexibly, and elegantly scales to meet the demands of even the largest and most complex organizations. A powerful rules engine and comprehensive exception handling features help minimize the impact on end users and IT teams alike.