

Search the blog


[Best practices Incident response](#) [Microsoft Incident Response](#) [Cybercrime](#)

3 min read

Patch me if you can: Cyberattack Series

By [Microsoft Incident Response](#)

June 29, 2023



Microsoft Security Experts

Microsoft Security Insights

Many organizations utilize third-party apps for identity security solutions to automate and unburden overtaxed IT admins from tedious tasks that employees can perform via self-service without IT assistance. But in September 2021, our researchers observed threat actors exploiting one such third-party app at several US-based entities. The vulnerability was publicly reported on September 6, 2021 as CVE-2021-40539 Zoho ManageEngine ADSelfService.¹ The application in question was a multifactor authentication, single sign-on, and self-service password management tool to help eliminate password reset tickets that create unnecessary, tedious work for IT admins. Bad actors exploited a patch vulnerability in the app, using it as an initial vector to gain a foothold in networks and perform additional actions including credential dumping, installing custom binaries, and dropping malware to maintain persistence. At the time of disclosure, RiskIQ observed 4,011 instances of these systems active and on the internet.

To learn more about this cyberattack series and how to protect your organization, please read the third [cyberattack series report](#). The report provides detailed information about the vulnerability, how it was exploited, and how organizations can mitigate the risk. It also includes recommendations for how organizations can improve their security posture to prevent similar attacks in the future.

Examining the remote ransomware attack

In the third installment of our ongoing Cyberattack Series, we examine this remote access ransomware attack and look at how [Microsoft Incident Response](#) thwarted it. We then delve further into the details with a timeline of events and how it all unfolded—using reverse engineering to learn where and when the threat actor first targeted the vulnerable server. We also explore the proactive steps that customers can take to prevent many similar incidents, and the actions necessary to contain and recover from attacks once they occur.

More than half of known network vulnerabilities found in 2021 were found to be lacking a patch. Plus, 68 percent of organizations impacted by ransomware did not have an effective vulnerability and patch management process, and many had a high dependence on manual processes versus automated patching capabilities. With today's threat landscape, it was only a matter of time before this zero-day vulnerability was exploited.

To compound the issue, the ways in which threat actors are working together now makes patch exploits more likely than ever before. Not only are attacks happening faster, they're more coordinated. We have also observed a reduction in the time between the announcement of a vulnerability and the commoditization of that vulnerability. Threat actors are organized and cooperating to exploit vulnerabilities faster, and this adds to the urgency that organizations face to patch exploits immediately.

The “commoditization” of vulnerabilities

While zero-day vulnerability attacks often initially target a limited set of organizations, they are quickly adopted into the larger threat actor ecosystem. This kicks off a race for threat actors to exploit the vulnerability as widely as possible before their potential targets install patches. Cybercrime as a Service or Ransomware as a Service websites routinely automate access to compromised accounts to ensure the validity of compromised credentials and share them easily. One set of cybercriminals will gain access to a compromised app then sell that access to multiple other bad actors to exploit.

The importance of cybersecurity hygiene

The most effective defenses against ransomware include multifactor authentication, frequent security patches, and Zero Trust principles across network architecture. Attackers usually take advantage of an organization's poor cybersecurity hygiene, from infrequent patching to failure to implement multifactor authentication.

Cybersecurity hygiene becomes even more critical as actors rapidly exploit unpatched vulnerabilities, using both sophisticated and brute force techniques to steal credentials, then obfuscating their operations by using open source or legitimate software. Zero-day exploits are both discovered by other threat actors and sold to other threat actors, then reused broadly in a short period of time leaving unpatched systems at risk. While zero-day exploitation can be difficult to detect, actors' post-exploit actions are often easier to notice. And if they're coming from fully patched software, it can act as a warning sign of a compromise and minimize impact to the business.

[Read the report](#) to go deeper into the details of the attack, including the threat actor's tactics, the response activity, and lessons that other organizations can learn from this case.

Examining a ransomware attack

Learn how Microsoft Incident Response thwarted a remote access ransomware attack.

[Read the detailed report >](#)

What is the Cyberattack Series?

With this Cyberattack Series, customers will discover how Microsoft incident responders investigate unique and notable exploits. For each attack story, we will share:

- How the attack happened.
- How the breach was discovered.
- Microsoft's investigation and eviction of the threat actor.
- Strategies to avoid similar attacks.

Read the first two blogs in the Cyberattack Series: [Solving one of NOBELIUM's most novel attacks](#) and [Healthy security habits to fight credential breaches](#).

Learn More

To learn more about Microsoft Security solutions, visit our [website](#). Bookmark the [Security blog](#) to keep up with our expert coverage on security matters. Also, follow us on LinkedIn ([Microsoft Security](#)) and Twitter ([@MSFTSecurity](#)) for the latest news and updates on cybersecurity.

¹[Threat actor DEV-0322 exploiting ZOHO ManageEngine ADSelfService Plus](#), Microsoft Threat Intelligence. November 8, 2021.

Source for all statistics in post: [Microsoft Digital Defense](#)

Related Posts





[Best practices](#)

[AI and machine learning](#)

[Microsoft Intune](#)

Jun 26

7 min read

Why endpoint management is key to securing an AI-powered future > >

With the coming wave of AI, this is precisely the time for organizations to prepare for the future. To be properly ready for AI, Zero Trust principles take on new meaning and scope. The right endpoint management strategy can help provide the broadest signal possible and make your organization more secure and productive for years to come.



[News](#)

[Email security](#)

May 19

3 min read

Cyber Signals: Shifting tactics fuel surge in business email compromise > >

Business email operators seek to exploit the daily sea of email traffic to lure victims into providing financial and other sensitive business information.



[Events](#)

[Security management](#)

[Microsoft Defender](#)

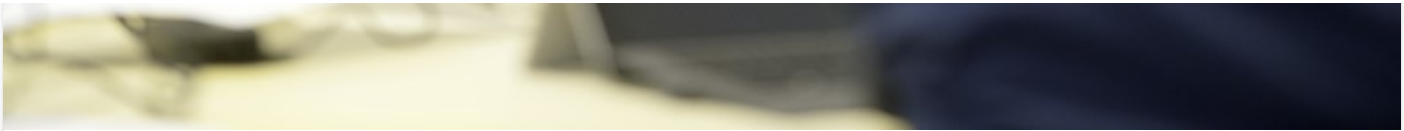
May 15

8 min read

Microsoft Security highlights from RSA Conference 2023 > >

At RSA Conference April 24 to 26, 2023, Microsoft Security shared solution news and insights. Watch Vasu Jakkal's keynote on-demand (video courtesy of RSA conference).





[News](#)
[Security management](#)

Mar 8
7 min read

International Women’s Day: The power of diversity to build stronger cybersecurity teams > >

On International Women’s Day, we celebrate the accomplishments of women in technology and reflect on our commitment to encouraging and supporting women in cybersecurity.

Get started with Microsoft Security

Microsoft is a leader in cybersecurity, and we embrace our responsibility to make the world a safer place.

Learn more

Connect with us on social



What's new

- Surface Laptop Studio 2
- Surface Laptop Go 3
- Surface Pro 9
- Surface Laptop 5
- Microsoft Copilot
- Copilot in Windows
- Explore Microsoft products
- Windows 11 apps

Microsoft Store

- Account profile
- Download Center
- Microsoft Store support
- Returns
- Order tracking
- Certified Refurbished

[Microsoft Store Promise](#)

[Flexible Payments](#)

Education

[Microsoft in education](#)

[Devices for education](#)

[Microsoft Teams for Education](#)

[Microsoft 365 Education](#)

[How to buy for your school](#)

[Educator training and development](#)

[Deals for students and parents](#)

[Azure for students](#)

Business

[Microsoft Cloud](#)

[Microsoft Security](#)

[Dynamics 365](#)

[Microsoft 365](#)

[Microsoft Power Platform](#)

[Microsoft Teams](#)

[Copilot for Microsoft 365](#)

[Small Business](#)

Developer & IT

[Azure](#)

[Developer Center](#)

[Documentation](#)

[Microsoft Learn](#)

[Microsoft Tech Community](#)

[Azure Marketplace](#)

[AppSource](#)

[Visual Studio](#)

Company

[Careers](#)

[About Microsoft](#)

[Company news](#)


[Privacy at Microsoft](#)


[Investors](#)

[Diversity and inclusion](#)

[Accessibility](#)

[Sustainability](#)

 [English \(United States\)](#)

 [Your Privacy Choices](#)

[Consumer Health Privacy](#)

[Sitemap](#) [Contact Microsoft](#) [Privacy](#) [Terms of use](#) [Trademarks](#) [Safety & eco](#) [Recycling](#) [About our ads](#) [© Microsoft 2024](#)