idea LOGICAL

LOGICAL TALK · March 2021 EDITION

Biggest Cyber Incident of 2021:

Exploitation of Microsoft Exchange “Zero-Day” Vulnerabilities

On March 2, 2021, Microsoft published several security updates after identifying four “Zero-Day” vulnerabilities. Security researcher Volexity reports that the activity may have started as early as January 6, 2021.

[Learn what is a “zero-day” vulnerability?]

What Was The Cybersecurity Emergency With Microsoft Exchange “Zero-Day” Vulnerability Hack?

On March 2, Microsoft released patches to tackle four severe vulnerabilities in Microsoft Exchange Server software. At the time, Microsoft said that the bugs were being actively exploited in “limited, targeted attacks.”

The attackers used the four newly discovered security vulnerabilities to break into Exchange email servers running on company networks, granting the attackers to steal data from a victim’s organization — such as email accounts and address books — and the ability to plant malware. When used together, the four vulnerabilities create an attack chain that can compromise vulnerable on-premise servers running Exchange 2013 and later.

Due to the severity of the attack, Microsoft released a patch for Windows 10, which has been discontinued since October 2020.

While fixes have now been issued, the scope of potential Exchange Server compromise depends on the speed and uptake of patches -- and the number of estimated victims continues to grow.

What Is Microsoft Exchange Used For?

Microsoft Exchange Server is used by the larger enterprise to small and medium-sized businesses worldwide. In simple terms, it is your regular outlook mailbox, calendar and integration with other collaborative solutions like Microsoft Teams, SharePoint, etc.

Who Is Responsible For Known Attacks Of Microsoft Exchange “Zero-Day” Vulnerabilities?

Microsoft says that attacks using the zero-day flaws have been traced back to HAFNIUM – a China state-sponsored threat actor. Microsoft believes the hacking group tries to steal information from a broad range of U.S.-based organizations, including law firms and defence contractors, but also infectious disease researchers and policy think tanks.

How Did Idealogical Handle The Microsoft “Zero-Day” Vulnerability Nightmare?

Andre de Lacerda - Technical Manager, Idealogical

“We came to know about the attack during the early a.m. hours of March 2, and we followed our Disaster Recovery Plan, which is custom-built for every Idealogical client for unforeseen emergencies exactly like this one”, said Andre de Lacerda, Technical Manager, Idealogical.

“We were one of the first group of IT teams to run the right patch within the first hour after the news of the zero-day vulnerability broke. For most clients, we were able to run the patch in about 30-40 minutes with a downtime of as little as 15 minutes. For a handful of clients whose days we couldn’t interrupt, we were able to run the patch in the same amount of time Afterhours”.

“We were able to protect our clients from this colossal attack because our servers were up-to-date. For MSPs or the IT departments whose servers were out of date, it will take them days or even weeks to run the patch”, Andre added.

Have You Uninstalled Adobe Flash Player Yet?

Adobe Flash Player, the household name for media playing software, reached its End of Life on December 31, 2020. Additionally, Adobe has started blocking Flash content from running in Flash Player from January 12, 2021.

What does End of Life mean?

End of life (EOL) in relation to software or hardware means that the vendor is ending support on the product or its version. This means the vendor will stop releasing maintenance and security patches and support for the software/ hardware. The vendors generally announce EOL to push their newer products or their more recent versions.

What are the platforms that have disabled Adobe Flash Player?

Most leading browsers have disabled Adobe Flash Player. Google Chrome, Microsoft Internet Edge, Microsoft Explorer, Mozilla Firefox and Apple Safari have disabled Adobe Flash Player.

What to do with your previously installed Adobe Flash Player?

Adobe Flash Player may remain on your system, and you may have to uninstall the software from your system manually. Uninstalling Flash Player is essential for your systems’ security as Adobe has stopped issuing any updates or security patches after January 12, 2021. Additionally, all major web browsers have disabled Adobe Flash Player from running any content from the EOL date.

How to uninstall Adobe Flash Player?

There are two ways of uninstalling Adobe Flash Player from your systems.

1. System Pop-ups: If your Adobe pop-up appears on your system, simply follow the uninstall instructions.
2. Manual Uninstall: Follow the Adobe guidance provided for Windows and Mac OS.

Superstar Of The Month - Darren Meunier

I appreciate the acknowledgment of hard work at Idealogical. I truly believe that awards are the culmination of having a great team; take away the team, and there will be no awards. While I am one of the more tenured employees at Idealogical, at 11 years, I believe that we have the right team over the years past. There is a tremendous amount of camaraderie and teamwork experienced every day, and every employee is happy to help others out at a moment’s notice.

The Idealogical team upholds our core values at every interaction, and we will look forward to continuing this trend.