

Introduction

Across the globe, people are becoming more and more dependent on technology as a way of mitigating the number of tasks we have to complete throughout the day. Many people don't take the time to ask themselves, "Is my data secured from an attack?" Though this isn't something that the average everyday person would constantly ask themselves, as we create new advancements related to technology, this question becomes one of imperative interest. In recent years, there has been a significant increase in ransomware attacks, targeting organizations of all shapes and sizes, from third-party digital vendors to international corporations like Microsoft and Google. Inside a ransomware attack, a malicious actor bypasses security measures to gain access into the target system and encrypts the data, temporarily withholding it from the user to access. In order to access this data again, the victim must pay the actor a certain amount of money, also known as a ransom, before a determined time before their data is either deleted or sold off. There are various methods Black Hats can use in order to bypass certain security measures that prevent this security measure, as well as disparities within the security, formally known as vulnerabilities. In the case of the ConnectWise cyberattack, launched in February of this year, a group of Black Hats were able to identify vulnerabilities in a product released from this company, causing disruptions among various institutions dependent on it. This blog will highlight the vulnerabilities, the attack vectors the Black Hats used in order to gain access, the protocols and applications that are affected by this attack, and the impact it left on the affected organizations.

Vulnerabilities and Attack Methods

The ConnectWise cyberattack can be classified as ransomware due to the method the actors used once they were able to obtain the data. Originally, ConnectWise was an information technology (IT) company that specialized in service management, automation, and remote support functionalities. This company released a product called ConnectScreen, known as ConnectWise Control, which served to help IT professionals manage and resolve technical issues efficiently. With features such as advanced encryption, customizable interfaces, and seamless integration, this product provided users with secure and reliable solutions for remote support. In February of 2024, ConnectWise received numerous complaints from institutions claiming that there were possible vulnerabilities within the system that needed to be addressed. These vulnerabilities were later determined to be CVE-2024-1709, which bypasses any authentication mechanism, and CVE-2024-1708, which authorized the Black Hats to execute malicious code remotely within the system (Fadilpašić, 2024). These security flaws impacted all servers that were currently running on the ConnectScreen 23.9.7 version of the application or any older models, which enabled the actors to deploy ransomware code all while extracting sensitive data. As more reports began to be filed, there was speculation that this attack was carried out by multiple parties from around the world. Many experts believe that this attack wasn't done by a single person but by what they call "en-mass exploitation" from various hacker groups, including the notorious LockBit ransomware gang (Brandt, 2024). After hearing note of these vulnerabilities, experts quickly worked on patching up these flaws and urged all of its consumers to update their systems as quickly as possible to avoid becoming a victim. An attack like this serves as a reminder of the inherent dangers of relying on technology without proper security

measures (Page, 2024). It highlights the importance of prioritizing vulnerability mitigation and the need for proactive measures that can notify the correct personnel once an attack is initiated.

Impact on Organizations

The aftermath of this cybersecurity attack left many organizations in hot water, having to tell their consumers that their data may have been compromised. Organizations that depended on ConnectWise for remote support in customer service experienced significant disruptions towards their daily operations. This is due to the fact that the perpetrators that infiltrated the system embedded ransomware codes that encrypted all the files within the system, rendering them inaccessible (Fadilpašić, 2024). This in turn resulted in some companies having to halt all operations, which led to financial losses and customer dissatisfaction. Alongside these operational delays, these organizations also noticed that sensitive data had been stolen. Stolen data, such as business information and medical records, are usually sold to Black Market vendors or used to amplify another attack (Brandt, 2024). Methods of attack such as this threaten not only the integrity and accessibility of the data but also expose innocent potential bystanders to potential risks. Once the brunt of the attack was mapped out and the security patch was circulating throughout the company, organizations had to compensate for recovery efforts with forensic investigations, data restoration, and the implementation of up-to-date security measures to prevent another attack such as this (Brandt, 2024). Despite ConnectWise releasing patches to address the exploited vulnerabilities that allowed this attack to happen, many companies failed to comply with the warnings, resulting in them becoming exposed in the attack. From an organization's perspective, an attack like this can be viewed as a learning lesson for what happens if security measures aren't up-to-date. The importance of having an incident response

plan that is effective in combating against cyber threats is crucial to the longevity of a company in today's era. This can also serve as a reminder of the evolving nature of cyber threats and how we as cybersecurity professionals need to implement good practices to deter actors from pursuing further.

Conclusion

The ConnectWise ransomware attack serves as a reminder that vulnerabilities present in commonly used items can be exploited and can cause damages to the consumer and organization. With the vulnerabilities exploited in ConnectWise's ConnectScreen product, malicious actors like the LockBit ransomware gang were able to bypass authentication security measures, remotely execute malicious code within the system, and steal sensitive data. The repercussions of this incident caused multiple disruptions, financial loss, and the compromise of consumer data across all that used the product. Other repercussions include the deployment of a forensics investigation to determine the cause, data restoration, and enhanced security measures in an attempt to prevent another attack such as this. Even though ConnectWise issued a patch update to the systems, many consumers failed to comply, resulting in a wider attack radius. Had these consumers taken action towards securing and updating their products, the attack would not have spread to how it initially was. Other organizations can learn from this attack by implementing good practices such as regularly updating security measures to prevent an attack like this on their own systems.

References

Page, Carly. “Hackers Are Exploiting ConnectWise Flaws to Deploy LockBit Ransomware, Security Experts Warn | TechCrunch.” *TechCrunch*, 23 Feb. 2024, techcrunch.com/2024/02/23/hackers-are-exploiting-connectwise-flaws-to-deploy-lockbit-ransomware-security-experts-warn/.

Sead Fadilpašić. “The ConnectWise Cyberattack Just Got a Whole Lot Worse.” *TechRadar*, TechRadar pro, 27 Feb. 2024, www.techradar.com/pro/security/the-connectwise-cyberattack-just-got-a-whole-lot-worse.

Sead Fadilpašić. “ConnectWise Remote Access Tool Hacked — Security Pros Are Saying It Is Bad, so Patch Now.” *TechRadar*, TechRadar pro, 22 Feb. 2024, www.techradar.com/pro/security/connectwise-remote-access-tool-hacked-security-pros-are-saying-it-is-bad-so-patch-now.

Brandt, Andrew. “ConnectWise ScreenConnect Attacks Deliver Malware.” *Sophos News*, 23 Feb. 2024, news.sophos.com/en-us/2024/02/23/connectwise-screenconnect-attacks-deliver-malware/?form=MG0AV3.

Nicolo, Leeann. “LockBit Linked to Exploitation of ConnectWise ScreenConnect.” *Coalitioninc.com*, 2024, www.coalitioninc.com/blog/lockbit-ransomware-connectwise-screenconnect?form=MG0AV3.