

VOL. 2

CYBER NEWS

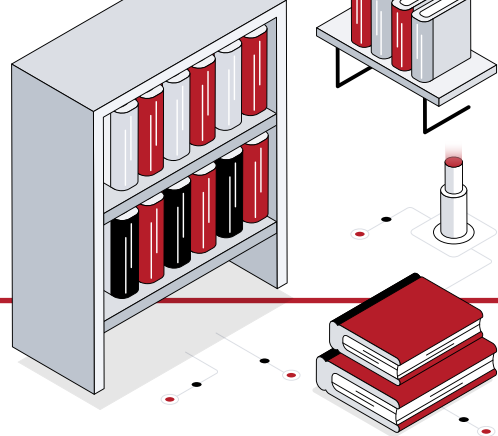
JOURNAL



Kapital Bank

2024

Table of Content



Cisco AnyConnect VPN: Ransomware attack on remote business infrastructure.....	03
Zero-day vulnerability on the Zoom platform: caused companies to become victims of espionage.....	04
Microsoft Teams accounts targeted by phishing attacks: internal data theft.....	05
Google Workspace Trojan attack: spying through Google Docs add-ons.....	06
The supply chain attack led to a massive data leak on the SaaS platform.....	07
New vulnerability discovered in Microsoft Exchange Server.....	08
A vulnerability was discovered in Adobe Acrobat Reader: Users' data is at risk!.....	09
Sources.....	10

Cisco AnyConnect VPN: Ransomware attack on remote business infrastructure

Recently, cyberattacks have increasingly targeted remote work-related systems.



Cybercriminals spread malicious files by imitating Cisco AnyConnect VPN software. When employees download this VPN software, malware enters the system and encrypts files on the target's computer. Cybercriminals demand a ransom to decrypt the files. Usually payments are requested through cryptocurrencies, so it becomes easier to hide the identity of cybercriminals.

Attacks of this type have increased dramatically in recent times, since later, in connection with the COVID-19 pandemic, remote work models began to become widespread.

How was this solved?

To prevent such attacks on companies, it is recommended to regularly update VPN programs, download software only from official and well-known sources, apply multi-factor authentication and increase the vigilance of users regarding social engineering and its types.

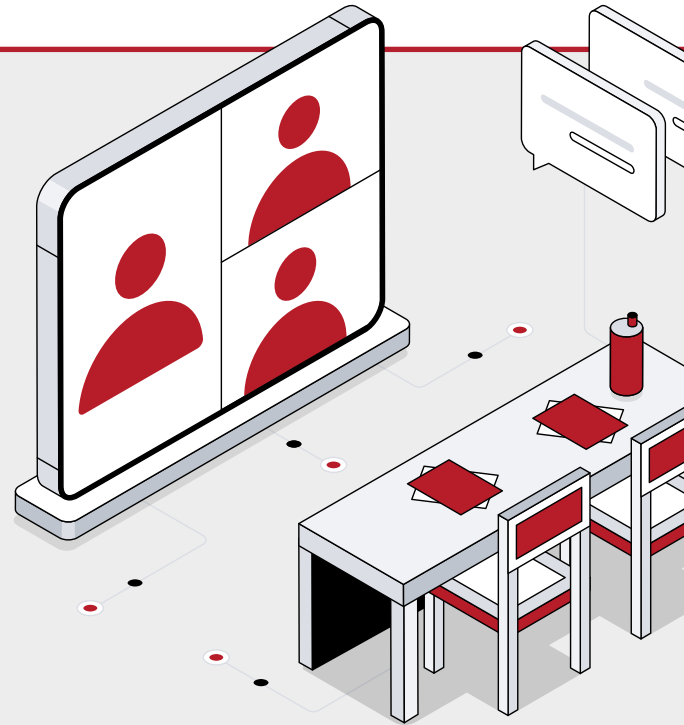
At the same time, it can help you avoid at least some damage from ransomware attacks by backing up data.



Zero-day vulnerability on the Zoom platform: caused companies to become victims of espionage

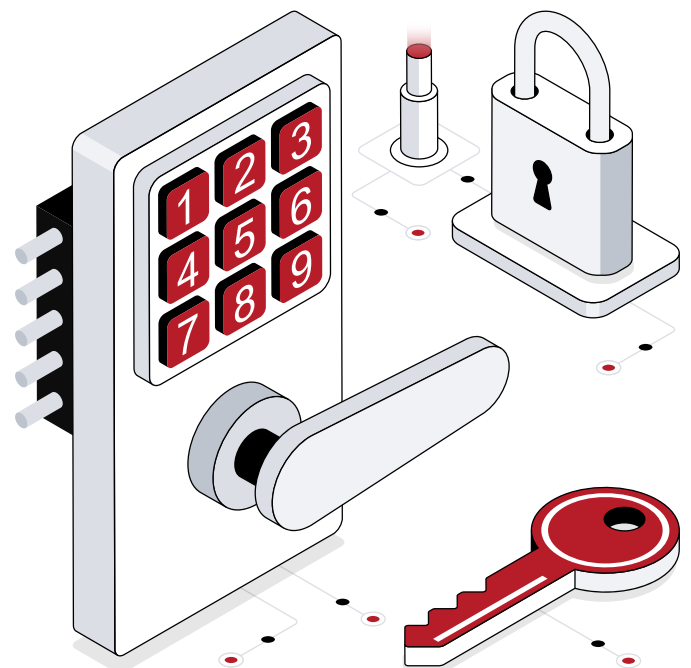
Zoom has become one of the most used video conferencing platforms, especially during the pandemic. However, this popularity did not go unnoticed by cybercriminals.

The newly discovered zero-day vulnerability allowed unauthorized access to Zoom conferences, making it possible for a number of companies to steal confidential information in this way. During this attack, cybercriminals were able not only to leak information by joining conferences directly, but also to install malicious programs on the participants' computers.

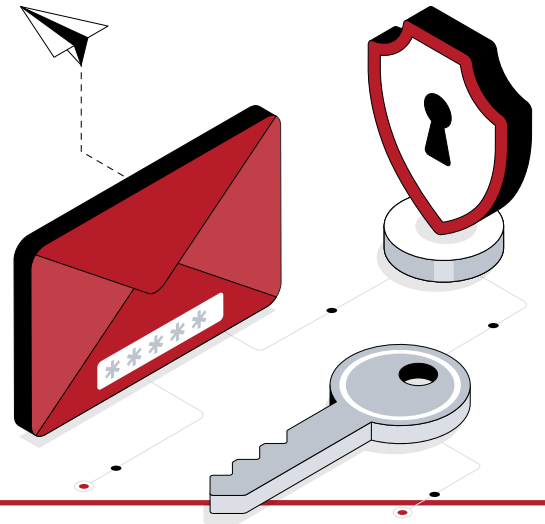


How could this problem be overcome?

Despite the fact that Zoom has released security updates (patch) and closed this gap, experts advise companies to create password-protected rooms for secure video conferences, strictly monitor the access control for participants and use only encrypted communication tools at meetings. And companies that do not take security measures can face serious data leaks and losses.

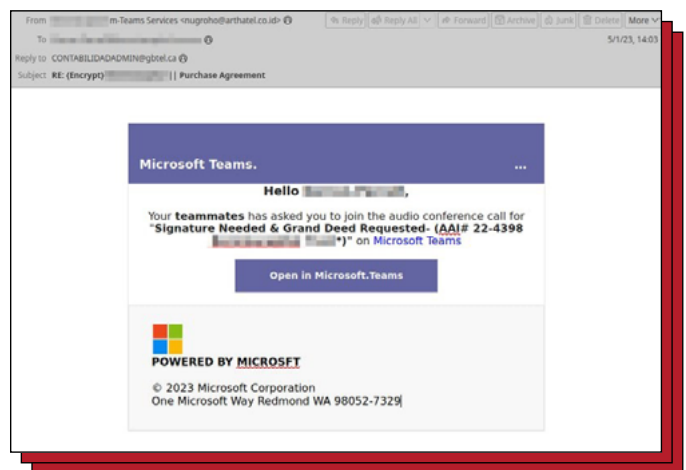


Microsoft Teams accounts targeted by phishing attacks: internal data theft



Microsoft Teams is a widely used collaboration and communication platform. Attacks through this platform are usually carried out with phishing emails or fake web login pages.

Hackers send users an emergency update or system-related warning to access Microsoft Teams and redirect victims to fake login pages. Here their login data is stolen, and after that cybercriminals gain access to the company's internal data.



Targeted companies may lose sensitive files, project information, and confidential correspondence stored in Microsoft Teams. As a result of attacks, transactions are disrupted, the reputation of companies is damaged. Microsoft security experts recommend the use of multi-factor authentication (MFA) and emphasize the importance of training employees to recognize phishing attacks. Thus, it is very important to consider alternative ways for safe communication .



Google Workspace Trojan attack: spying through Google Docs add-ons

The Google Workspace logo is centered in the upper half of the page. It features the word "Google" in its signature multi-colored font (blue, red, yellow, green, blue) followed by the word "Workspace" in a plain, grey, sans-serif font. The logo is flanked by two stylized, colorful shapes that resemble the Google logo's characteristic rounded corners, one on the left and one on the right.

Google Workspace is widely used as a productivity and collaboration tool for many businesses. But through the recently discovered trojan virus, a new threat has appeared on the platform.

The malware presents itself as Google Docs add-ons and starts malicious activities when users install these add-ons. The Trojan virus gives full control over the target's system, and personal data, files are stolen. Hackers monitor the activity of users, collect sensitive information and place backdoors on systems.

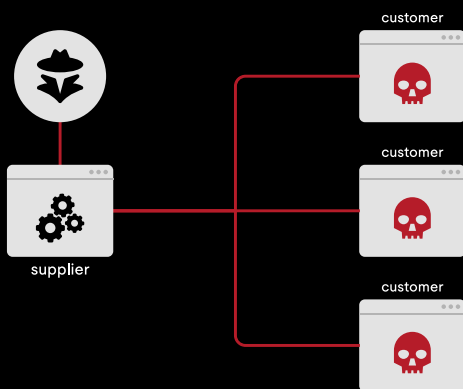
Large amounts of data can be stolen or deleted during an attack. Google has released security updates in response to this attack/ Experts recommend that organizations use only approved add-ons, limit storage of sensitive documents, and strengthen security configurations.

It is important that companies constantly monitor to protect their systems with additional security monitoring.



The supply chain attack led to a massive data leak on the SaaS platform

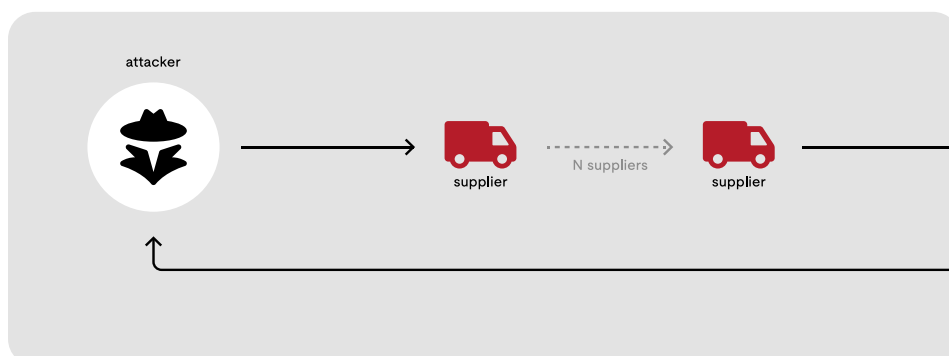
SaaS (Software-as-a-Service) platforms have become one of the main services of many companies, but serious problems arise with their security. Recently, a supply chain attack occurred on one of the SaaS platforms. Hackers had placed malicious code in libraries that were used by third parties who received the services of this platform. Cybercriminals, who gained access to the platform through this code, stole the accounts and personal data of thousands of users.



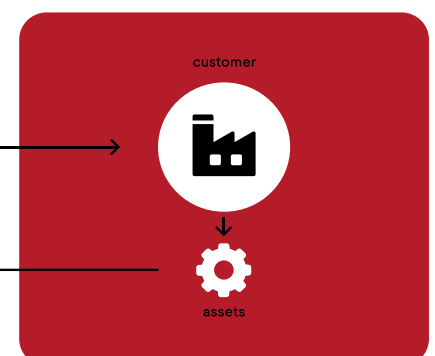
As a result of this attack, data in the financial and health sectors, in particular, were at risk. Supply chain attacks are complex because they do not originate directly from the platform itself, but from third-party resources. The security systems of the platforms can sometimes have difficulty detecting such attacks.

Experts emphasize that companies should more carefully evaluate their business relationships with third-party providers and conduct security audits. Identifying and eliminating vulnerabilities in the supply chain is crucial for protecting a company's information.

SUPPLIER ATTACK



CUSTOMER APT ATTACK



New vulnerability discovered in Microsoft Exchange Server

In February 2024, a critical vulnerability (CVE-2024-21410) was discovered in Microsoft Exchange Server. This vulnerability has been actively exploited by cybercriminals. By performing a Net-NTLMv2 “hash relay,” attackers were able to obtain the same privileges as the legitimate users. NTLM (NT LAN Manager) is an authentication protocol used by Microsoft in network environments.

Microsoft Exchange Server Elevation of Privilege Vulnerability
CVE-2024-21410
Security Vulnerability

Released: Feb 13, 2024 Last updated: Feb 14, 2024

Assigning CNA: Microsoft

[CVE-2024-21410](#)

Impact: Elevation of Privilege Max Severity: Critical

CVSS:3.1 9.8 / 9.1

It encrypts users' data and sends it to the server. "Relay" refers to cybercriminals forwarding authentication data (hashes) from one system to another. Specifically, cybercriminals used NTLM clients such as Outlook to steal these hashes and compromise the Exchange Server. Using this method, they performed various actions on behalf of the victims.

The result of weakness

As a result of this exploit, cybercriminals gained unauthorized access to information in the companies' email systems. They also stole confidential correspondence and critical information, leading to significant data loss for the companies. This has led to a large loss of data for companies.

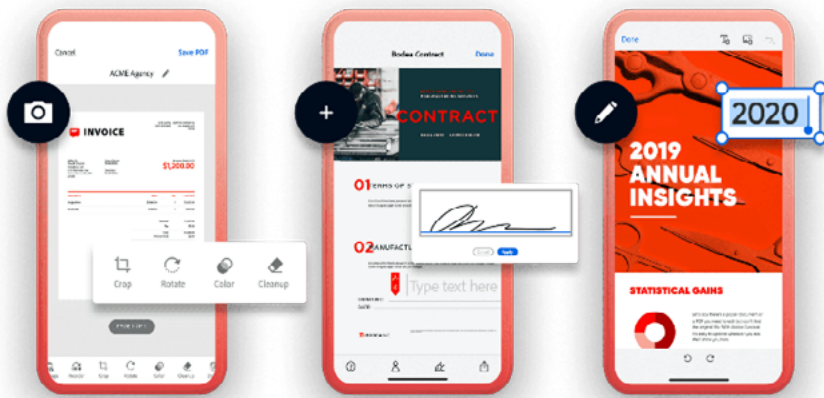


How to solve the problem

After Microsoft discovered this vulnerability, it released a security update for Exchange Server 2019 called “Cumulative Update 14” (CU14). This upgrade helps prevent future attacks by creating additional defense. Microsoft has recommended that all users urgently apply this update. The vulnerability has been fixed since the update was applied.



A vulnerability was discovered in Adobe Acrobat Reader: **Users' data is at risk!**



Recently, a serious vulnerability was discovered in Adobe Acrobat Reader. This vulnerability is identified by the code CVE-2024-41896 and is known as “use after free.” Hackers were able to exploit this vulnerability to launch malicious code on target devices remotely.

The vulnerability was discovered by cybersecurity expert Haifei Li. He created a platform called EXPMON, which helps identify new zero-day vulnerabilities. This platform detects gaps during the loading of various files. The expert notes that the exploitation of this vulnerability has already begun, but so far, these malicious PDF files are used only to disable target devices. This, in itself, indicates that the vulnerability has not yet fully escalated.





Impact of vulnerability

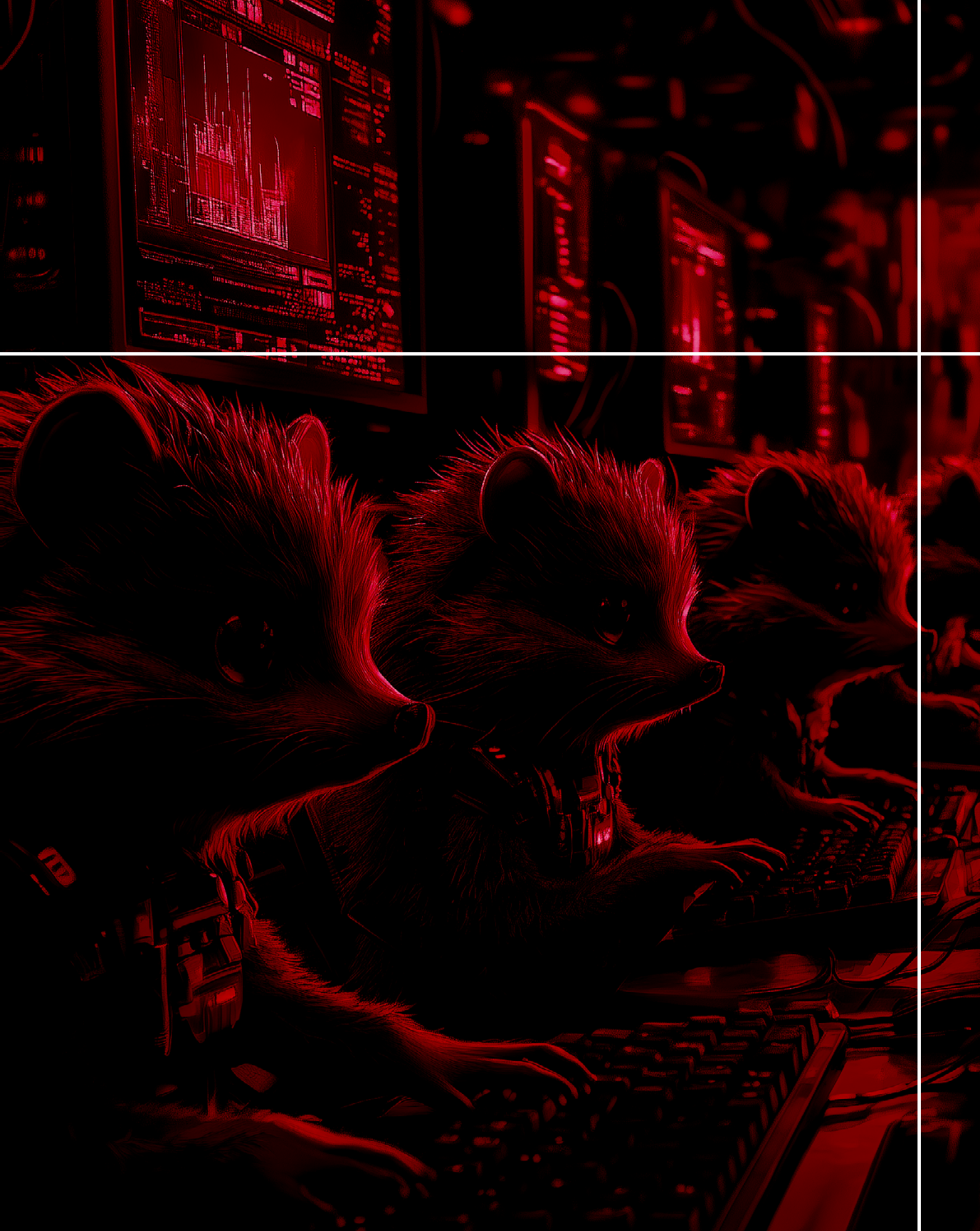
Hackers who exploit this vulnerability can disable target devices, potentially damaging users' data and systems. Thus, cybercriminals can take advantage of this vulnerability to install malicious programs that may have a more serious impact on the system.

Adobe has released security updates to address this issue and has advised all users to update their software immediately. These updates help eliminate vulnerabilities and prevent potential attacks.

Sources

-  www.truesec.com/hub/blog/akira-ransomware-and-exploitation-of-cisco-anyconnect-vulnerability-cve-2020-3259
-  www.securityhq.com/blog/critical-zero-day-vulnerability-in-zoom/
-  www.techtarget.com/searchsecurity/tip/Microsoft-Teams-phishing-attacks-and-how-to-prevent-them
-  www.techradar.com/news/google-docs-is-being-weaponized-by-hackers
-  www.adaptive-shield.com/academy/saas-attack-surface/
-  www.securityweek.com/microsoft-warns-of-exploited-exchange-server-zero-day/
-  www.techradar.com/pro/security/adobe-acrobat-reader-has-a-serious-security-flaw-so-patch-now





Kapital Bank