HC3: Alert

October 4, 2023 TLP:CLEAR Report: 202310041400

Securing Remote Access and Management Software

Executive Summary

Cybersecurity and law enforcement agencies such as CISA, MS-ISAC, CIS, and the FBI have been reporting on increased misuse of remote access software to target organizations and critical infrastructure sectors. For implications to the Healthcare and Public Health (HPH) sector, remote access solutions keep healthcare professionals connected while also providing increased flexibility and convenience. But the same solutions used to operate, maintain, and secure healthcare systems and networks can also be turned against their own infrastructure. Mitigating the risk associated with them is not as simple as deploying a patch or reconfiguring an application.

Common Remote Access Solutions in the HPH Sector

In the healthcare sector, remote access tools are crucial for providing efficient and secure access to patient data, such as Electronic Protected Health Information (ePHI) and facilitating remote patient care. Below are some common remote access tools used in the healthcare sector. It is important to note that healthcare organizations need to ensure that these remote access tools are implemented and used in compliance with relevant healthcare regulations and privacy laws, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States.

- **Virtual Private Networks (VPNs):** VPNs allow healthcare professionals to securely access patient data and systems remotely. They establish an encrypted connection between the user's device and the healthcare organization's network, ensuring data privacy and protection.
- **Remote Desktop Software:** Remote desktop software, such as Remote Desktop Protocol (RDP) or Virtual Network Computing (VNC), enables healthcare professionals to access their office computer remotely. It allows them to view the desktop, access files, and use software as if they were physically present at their office.
- **Telehealth Platforms:** Telehealth platforms provide a range of remote access tools for virtual patient care, including video-conferencing, electronic health records (EHR) integration, and collaborative features. These platforms enable healthcare providers to conduct virtual consultations, monitor patients remotely, and share medical information securely.
- **Secure Messaging Apps:** Secure messaging apps allow healthcare professionals to communicate and share patient information securely. These tools provide end-to-end encryption, authentication, and other security measures to ensure the confidentiality and integrity of sensitive data.

Remote Access Software/ Remote Access Monitoring and Management Solutions Targeting

Remote access, monitoring, and management solutions play crucial roles in the healthcare sector. Remote access software enables healthcare professionals to access and control computer systems or devices located at a different physical location. By using this software, healthcare providers can securely connect to remote computers, access patient records, collaborate with colleagues, and provide remote consultations. Security agencies and law enforcement have highlighted that cyber threat actors are increasingly co-opting these same tools for easy and broad access to victim systems. Since remote access software is used by organizations for legitimate purposes, its use is frequently not flagged as malicious by security tools or processes.

Common threat actor TTPs for targeting remote access solutions:

- **Exploiting Vulnerabilities:** Threat actors may exploit vulnerabilities in remote access software to gain unauthorized access to healthcare systems and data. This could include exploiting software bugs, weak passwords, or configuration errors. In fact, healthcare organizations have been increasingly targeted by cyberattacks exploiting remote access vulnerabilities.
- **Brute-Force Attacks:** Threat actors may attempt to gain access to remote systems by launching brute-force attacks, where they systematically guess usernames and passwords until they find the correct combination. This method is commonly used against remote access software and can be particularly damaging if successful in the healthcare sector.
- **Social Engineering:** Threat actors may utilize social engineering techniques to trick healthcare professionals into submitting their login credentials or providing access to their remote access software. Phishing emails, fake support calls, or even impersonating IT personnel are some common social engineering methods used to target individuals in the healthcare sector.
- **Ransomware Attacks:** Threat actors may deploy ransomware onto healthcare systems through compromised remote access software. Once the ransomware is activated, it can encrypt critical healthcare data, leading to significant disruptions in patient care and potentially compromising sensitive information.

Threat Actor Targeting of Remote Access Solutions

In recent years, there have been several notable cybersecurity incidents involving malicious targeting of remote access software in the healthcare sector. These attacks often aim to exploit vulnerabilities in the software or gain unauthorized access to sensitive patient information. Here are a few notable examples:

- **Operation Emmental:** This cybercriminal operation targeted remote access systems and online banking applications, attempting to compromise users' personal information, including credentials and banking details. Though not limited to the healthcare sector, healthcare organizations were among the victims.
- **Botnet Attacks:** Cybercriminals have also utilized botnets to target remote access software in the healthcare sector. Botnets are networks of infected computers controlled by a central attacker. In 2015, the healthcare sector experienced an increase in botnet attacks aimed at compromising remote access systems.
- **Ransomware Incidents:** Ransomware attacks in the healthcare sector often exploit vulnerabilities in remote access software as an entry point. Attackers encrypt critical data and demand a ransom to restore access. The WannaCry and NotPetya outbreaks in 2017 were notable examples that affected healthcare organizations worldwide.
    - **Notable:** AvosLocker, a ransomware-as-a-service (RaaS), first spotted in 2021, uses the remote administration tool AnyDesk to connect to victim machines. AnyDesk is a proprietary software platform allowing users to remotely access another network environment. The application was initially released in 2015 and is widely used in the healthcare sector. The AvosLocker actors can get around security measures by utilizing a combination of Windows Safe Mode and AnyDesk to allow continuous remote access to the victim. After safe mode security functions were disabled, the threat actors can effecively deploy the ransomware variant; this variant can also be deployed in safe mode.

HC3: Alert

October 4, 2023 TLP:CLEAR Report: 202310041400

There are several advanced persistent threat (APT) groups that have been known to target the healthcare sector and specifically focus on remote access software. Here are a few examples:

- **APT29 (also known as "Cozy Bear" or "The Dukes"):** This Russia-based APT group has targeted healthcare organizations and government entities worldwide. They have been observed using remote access tools to gain unauthorized access to systems and conduct espionage activities.
- **APT32 (also known as OceanLotus or APT-C-00):** This Vietnam-based APT group has been known to target healthcare organizations in Southeast Asia. They have used remote access software to compromise systems, steal sensitive data, and carry out espionage activities.
- **APT41:** This China-based APT group has targeted various industries, including healthcare, using a wide range of techniques. They have been known to exploit vulnerabilities in remote access software to gain unauthorized access and exfiltrate data.

Recommendations (Mitigations)

It is important for healthcare organizations to stay vigilant and proactive in their cybersecurity efforts to protect their remote access and management software from potential threats. To mitigate these threats, cybersecurity and law enforcement agencies recommend that healthcare organizations should adopt robust security practices. For mitigations and more information on securing remote access software, please see the MS-ISAC “Guide To Securing Remote Access Software” listed in the reference section.

It is important for healthcare organizations to stay vigilant and proactive in their cybersecurity efforts to protect their remote access and management software from potential threats. Healthcare organizations should adopt robust security practices, including:

- **Utilize strong authentication methods:** Implement multi-factor authentication (MFA) to ensure that only authorized individuals can access remote systems. This can involve using a combination of passwords, biometrics, smart cards, or tokens for authentication.
- **Regularly update and patch software:** Keep remote access software and other related applications up to date with the latest security patches. Regularly check for software updates and apply them promptly to protect against known vulnerabilities.
- **Implement network segmentation:** Isolate sensitive healthcare systems from other networks by implementing network segmentation. This way, even if an unauthorized user gains access to one part of the network, they will not be able to navigate through the entire system.
- **Use strong encryption:** Implement strong encryption protocols, such as Transport Layer Security (TLS), to protect data transmitted over remote access connections. This prevents unauthorized individuals from intercepting and accessing sensitive data.
- **Monitor and log remote access activities:** Implement logging and monitoring mechanisms to track remote access activity. Analyzing logs can help identify any suspicious or unauthorized activities and allow for a timely response.
- **Implement access controls and permissions:** Ensure that remote access is provided only to necessary personnel, and strictly limit privileges based on role-based access control (RBAC) principles. Regularly review and update access permissions based on individual responsibilities and requirements.
- **Conduct regular security training and awareness programs:** Educate healthcare staff about the risks associated with remote access software and train them on best practices to mitigate those risks. This can include teaching about phishing attacks, social engineering, and the importance of

strong passwords.

- **Establish incident response protocols:** Develop and document an incident response plan to effectively respond to any security incidents related to remote access. This helps to minimize the impact of a potential breach and allows for a swift and efficient recovery process.
- **Regularly audit and assess security controls:** Conduct periodic audits and vulnerability assessments to identify any weaknesses in remote access security measures. This allows for proactive remediation of vulnerabilities before they can be exploited.
- **Engage with trusted vendors:** Choose remote access software from reputable vendors who prioritize security and provide regular updates and patches. Conduct thorough due diligence before selecting a vendor to ensure their software meets the necessary security requirements.
- Educating staff members about the risks of social engineering attacks and providing training on how to identify and respond to suspicious requests.

Relevant HHS Reports

202306081300_Types of Threat Actors That Threaten Healthcare_TLPCLEAR (hhs.gov) (June 8, 2023)

References

Guide to Securing Remote Access Software (cisa.gov) (June 6, 2023)

HIPAA Compliant Remote Access Software (hipaajournal.com)

HC3 Guidance Explores Cyber Threat Actors Targeting Healthcare (healthitsecurity.com) (June 12, 2023)

Ransomware Spotlight: AvosLocker - Nachrichten zum Thema Sicherheit - Trend Micro DE (April 4, 2022)

New Medical Hijack Attacks Are Targeting Hospital Devices - Medical Design and Outsourcing (June 27, 2016)

APT29, IRON RITUAL, IRON HEMLOCK, NobleBaron, Dark Halo, StellarParticle, NOBELIUM, UNC2452, YTTRIUM, The Dukes, Cozy Bear, CozyDuke, SolarStorm, Blue Kitsune, Group G0016 | MITRE ATT&CK®

APT32, SeaLotus, OceanLotus, APT-C-00, Group G0050 | MITRE ATT&CK®

APT41, Wicked Panda, Group G0096 | MITRE ATT&CK®

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback