PSTA
PUBLIC SAFETY THREAT ALLIANCE
PUBLIC SAFETY ISAO

THREAT ADVISORY

TLP:CLEAR

Guide To Securing Remote Access Software

Disclosure Protocol: Clear — Disclosure is not limited
Date of Writing: June 12, 2023

Overview

The Cybersecurity and Infrastructure Security Agency (CISA) released a Guide to Securing Remote Access Software detailing methods for detecting and mitigating the growing threat of cyber threat actors targeting remote access software.

Remote access software is commonly used across public and private IT networks, as it provides a proactive and flexible approach for organizations to remotely oversee networks, computers, and other devices. Unfortunately, the capabilities of remote access software are also heavily favored by almost all cyber threat groups we have observed targeting public safety. When remote access software does not have proper monitoring and flags for nefarious activity, threat actors are able to use the tools to establish broad network access while going undetected.

In addition to targeting the remote software applications, adversaries heavily attack remote service protocols themselves. Since January 2022, we have observed at least 13 different attributed threat actors abusing remote services to gain initial access to public safety environments. Adversaries used tools like Windows Remote Desktop Protocol (RDP) and Server Message Block (SMB) to move across public safety networks and access new aspects of victim environments.

Details and technical guidance, such as the associated tactics, techniques, and procedures (TTPs) and detection and mitigation strategies can be found in the joint advisory.

Malicious Use of Remote Access Software & Services

The practice of targeting remote access software and remote services remains prevalent, and is in the top five methods by which adversaries access public safety victims. Threat actors desire these services because they:

- **Are hard to detect**. Since remote tools were created for legitimate use, anti-malware or endpoint and detection and response may not alert security teams when threat actors abuse remote access software in target environments.
- **Do not require extensive capability development**. Threat actors do not need to use or purchase developed remote access trojans (RAT) or other custom malware during engagements. Several vendors of remote access software allow free trials, and many victims often have existing remote protocols unsecured or open to the internet.
- **May allow bypassing software management control policies**. Even if user access controls (UACs) are put in place by system administrators or security teams, remote access software can act as a self-contained portable executable and let threat actors avoid administrative access restrictions.

- **Could allow adversaries to bypass firewall rules**. Several remote access applications offer end-to-end encryption. By creating an encrypted outbound or inbound connection, firewalls are unable to detect the download of files that would normally be caught in plaintext network traffic.
- **Can facilitate multiple cyber intrusions**. Managed Service Providers (MSPs) use remote access software to manage and monitor multiple customer environments at the same time. This is no different for threat actors. They are able to conduct multiple cyber intrusions all from the same graphical user interface (GUI), greatly expanding threat actors' operational capabilities.

Associated Tactics, Techniques, & Procedures (TTP)

For a full list of TTPs associated with remote access software, please refer to the attached Guide To Securing Remote Access PDF.

Detection

In order to properly detect the use of remote access software in an environment, it is necessary to create a security baseline of normal network and host activity within a monitored environment. By creating a baseline it can be easier for security teams to detect anomalous activity in a given environment. Host-based detection tools such as EDRs have the ability to monitor for remote access software. The following are commonly used remote access software used by threat actors who target public safety organizations:

- ConnectWise Control (formerly ScreenConnect)
- Anydesk
- Remote Utilities
- NetSupport
- Splashtop
- Atera
- TeamViewer
- Pulseway
- RemotePC
- Kaseya
- GoToMyPC
- N-Able
- Bomgar
- Zoho Assist

Recommended Mitigation Controls

The authoring organizations encourage network defenders to:

- Implement best practices to block phishing emails. See CISA's Phishing Infographic[1] for more information.
- Audit remote access tools on your network to identify currently used and/or authorized RMM software.
- Review logs for execution of RMM software to detect abnormal use of programs running as a portable executable.
- Use security software to detect instances of RMM software only being loaded in memory.
- Implement application controls to manage and control execution of software, including allowlisting RMM programs.

[1] https://www.cisa.gov/sites/default/files/publications/phishing-infographic-508c.pdf

    - See NSA's Cybersecurity Information sheet Enforce Signed Software Execution Policies[2] for more information.
    - Application controls should prevent both installation and execution of portable versions of unauthorized RMM software.
- Require authorized RMM solutions only be used from within your network over approved remote access solutions, such as virtual private networks (VPNs) or virtual desktop interfaces (VDIs).
- Block both inbound and outbound connections on common RMM ports and protocols at the network perimeter.
- Implement a user training program and phishing exercises to raise awareness among users about the risks of visiting suspicious websites, clicking on suspicious links, and opening suspicious attachments. Reinforce the appropriate user response to phishing and spearphishing emails.

[2] https://media.defense.gov/2019/Sep/09/2002180334/-1/-1/0/Enforce%20Signed%20Software%20Execution%20Policies%20-%20Copy.pdf

Appendix A: Assessment and Response Standard Operating Procedures

Levels of Analytic Confidence

High Confidence	Moderate Confidence	Low Confidence
Generally indicates judgments based on high-quality information, and/or the nature of the issue makes it possible to render a solid judgment. A "high confidence" judgment is not a fact or a certainty, however, and still carries a risk of being wrong.	Generally means credibly sourced and plausible information, but not of sufficient quality or corroboration to warrant a higher level of confidence.	Generally means questionable or implausible information was used, the information is too fragmented or poorly corroborated to make solid analytic inferences, or significant concerns or problems with sources existed.

Appendix B: Traffic Light Protocol for Disclosure

As part of the PSTA, agencies and other members are encouraged to share their own cybersecurity threat experiences to improve the awareness and readiness of the overall group. Submitting agencies should stipulate the level of disclosure required for their submissions according to the PSTA Traffic Light Protocol (TLP), based upon the CISA Traffic Light Protocol guidance, which helps all members submit and leverage insights while being respectful of the submitting agency's preferences.

RED: Restricted to the immediate PSTA participants only

- **When should it be used?** Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.
- **How may it be shared?** Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.

GREEN: Restricted to the community

- **When should it be used?** Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.
- **How may it be shared?** Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.

AMBER: Restricted to participants' organizations

- **When should it be used?** Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
- **How may it be shared?** Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. TLP:AMBER+STRICT Restricts sharing to the organization only.

CLEAR: Disclosure is not limited

- **When should it be used?** Sources may use TLP: CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.
- **How may it be shared?** Subject to standard copyright rules, TLP: CLEAR information may be distributed without restriction.

TLP: CLEAR