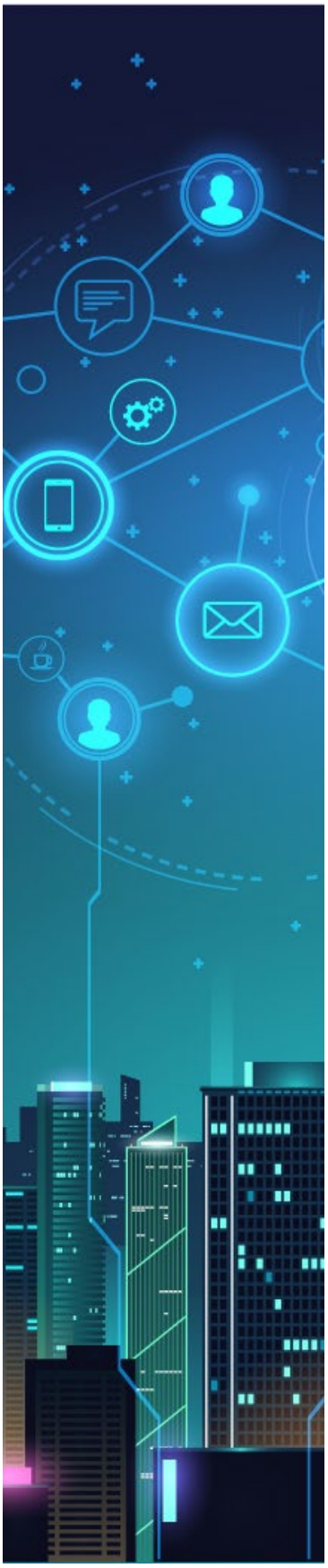
TLP:CLEAR

GUIDE TO SECURING REMOTE ACCESS SOFTWARE

Publication: June 6, 2023

TABLE OF CONTENTS



OVERVIEW: REMOTE ACCESS SOFTWARE

Remote access software and tools comprise a broad array of capabilities used to maintain and improve IT, operational technology (OT), and industrial control systems (ICS) services; they allow a proactive and flexible approach for organizations to remotely oversee networks, computers, and other devices. Remote access software, including remote administration solutions and remote monitoring and management (RMM), enables managed service providers (MSPs), software-as-a-service (SaaS) providers, IT help desks, and other network administrators to remotely perform several functions, including gathering data on network and device health, automating maintenance, PC setup and configuration, remote recovery and backup, and patch management.

Remote access software enables a user to connect to and access a computer, server, or network remotely.

- **Remote administration solution** is software that grants network and application access and administrative control to a device remotely.
- **Remote monitoring and management** is an agent that is installed on an endpoint to continuously monitor a machine or system's health and status, as well as enabling administration functions.

Legitimate use of remote access software enables efficiency within IT/OT management—allowing MSPs, IT help desks, and other providers to maintain multiple networks or devices from a distance. It also serves as a critical component for many business environments, both small and large empowering IT, OT, and ICS professionals to troubleshoot issues and play a significant role in business continuity plans and disaster recovery strategies. [1] However, many of the beneficial features of remote access software make it an easy and powerful tool for malicious actors to leverage, thereby rendering these businesses vulnerable.

This guide, authored by the Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Federal Bureau of Investigation (FBI), Multi-State Information Sharing & Analysis Center (MS-ISAC), and Israel National Cyber Directorate (INCD), with contributions from private sector partners listed on page 10, provides an overview of common exploitations and associated tactics, techniques, and procedures (TTPs). It also includes recommendations to IT/ OT and ICS professionals and organizations on best practices for using remote capabilities and how to detect and defend against malicious actors abusing this software.

MALICIOUS USE OF REMOTE ACCESS SOFTWARE

Remote access software provides IT/OT teams with flexible ways to detect anomalous network or device issues early on and proactively monitor systems. Cyber threat actors are increasingly co-opting these same tools for easy and broad access to victim systems. While remote access software is used by organizations for legitimate purposes, its use is frequently not flagged as malicious by security tools or processes. Malicious actors exploit this by using remote access software to establish network connections through cloud-hosted infrastructure while evading detection. This type of intrusion falls into the category of living off the land (LOTL) attacks, where inherently malicious files, codes, and scripts are unnecessary, and cyber threat actors use tools already present in the environment to sustain their malicious activity. For additional information and examples of LOTL attacks, see the joint Cybersecurity Advisory People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection.

RMM software in particular has significant capabilities to monitor or operate devices and systems as well as attain heightened permissions, making it an attractive tool for malicious actors to maintain persistence and move laterally on compromised networks. This enables MSPs or IT help desks to monitor multiple devices and networks at once, however these same features also make managing multiple intrusions easier for cyber threat actors. In this way, remote access software has become a common, high-value instrument for cyber threat actors, especially ransomware groups. Small- and mid-sized businesses rely on MSPs and the use of various types of remote access software to supplement their own IT, OT, and ICS infrastructures, and scale network environments without having to develop those capabilities internally. This makes businesses that much more vulnerable to service provider supply chain compromises, exploitation, or malicious use of remote capabilities.

Remote access software is particularly appealing to threat actors because the software:

- **Does not always trigger security tools.** Remote access software is often used for legitimate purposes, so it generally blends into the environment and does not trigger antivirus (AV), antimalware, or endpoint detection and response (EDR) defenses. RMM software is signed with valid code signing certificates issued by trusted certificate authorities, meaning that it will not appear inherently suspicious to AVs and EDRs. Often RMM install paths are excluded from EDR inspection.
- **Does not require extensive capabilities development.** Remote access software enables cyber threat actors to avoid using or developing custom malware, such as remote access trojans (RATs). The way remote access products are legitimately used by network administrators is similar to how malicious RATs are used by threat actors. [2]
- **May allow actors to bypass software management control policies.** While a bypass or exclusion can be required, remote access software also can be downloaded as self-contained, portable executables that enable actors to bypass both administrative privilege requirements and software management control policies.

  > **Note:** Portable executables launch within the user's context without installation. Additionally, because the use of portable executables often does not require administrator privileges, they can allow execution of other unapproved software, even if risk management controls may be in place to audit or block the same software's installation on the network. Threat actors can leverage a portable executable with local user rights to attack other vulnerable machines within the local intranet or establish long-term persistent access as a local user service.

- **Could allow actors to bypass firewall rules**. In addition to bypassing software management controls, many remote management agents use end-to-end encryption. This could allow a threat actor to download files that would typically be detected and blocked at the firewall.
- **Can facilitate multiple cyber intrusions**. Remote access software enables threat actors to manage multiple intrusions at once. In addition, initial access brokers may sell network access to many different cybercriminals, enabling multiple intrusions to the same network, as well as expanding the reach and ability of these cyber threat actors. If these actors first compromise an MSP, they could gain access to a large

number of the affected MSP's customers' networks and data.

ASSOCIATED TTPS

Cyber threat actors use remote access software for initial access, maintaining persistence, deploying additional software and tools, lateral movement, and data exfiltration. As such, remote access software— and RMM in particular—is often used by cybercriminals in ransomware incidents, and in certain APT campaigns. For an example of APT usage, see the joint Cybersecurity Advisory Iranian Government- Sponsored Actors Conduct Cyber Operations Against Global Government and Commercial Networks

Before leveraging remote access software as part of an intrusion, cyber actors may exploit vulnerable software. This may include exploiting legitimate servers that are then leveraged for malicious purposes. It may also include general network exploitation activities such as installing or placing remote access client software for persistence. Threat actors may also obtain legitimate, compromised remote access software credentials that ultimately enable them to exercise control over remote endpoints associated with the compromised account. Once initial access is obtained threat actors often use PowerShell or similar command line tools to silently deploy the RMM agent. Often, threat actors leverage multiple RMM mechanisms at once. Sometimes malicious actors also use RMM software in concert with commercial penetration testing tools such as Cobalt Strike or remote access malware to enable multiple, often redundant, forms of access to ensure persistence.

Threat actors use remote access software to perform multiple functions and carry out several commonly associated TTPs (e.g. credential dumps and escalating privileges.) See Table 1 for common tactics and techniques mapped to the MITRE ATT&CK® for Enterprise framework, version 13. **Note**: For assistance with mapping threat activity to the MITRE ATT&CK framework, see CISA's Best Practices for MITRE ATT&CK Mapping Guide and Decider Tool. MITRE also provides tactics and techniques specific to ICS, which can be found in the ICS Matrix.

Table 1: Common Threat Actor MITRE ATT&CK Tactics and Techniques

RESOURCE DEVELOPMENT		
Technique Title	ID	Use
Obtain Capabilities: Tool	T1588 .002	Threat actors can obtain software capabilities by buying, stealing, or downloading tools and using them for capabilities other than their intended use.
INITIAL ACCESS		
Technique Title	ID	Use
External Remote Services	T1133	Threat actors exploit externally-facing remote services, such as virtual private networks (VPNs), to enable initial access and persistence into a network from remote locations.
Supply Chain Compromise	T1195	Threat actors manipulate legitimate RMM software with modified versions.
Phishing	T1566	Threat actors have used phishing campaigns to lead victims to download legitimate RMM software. For more information, see the joint Cybersecurity Advisory Protecting Against Malicious Use of Remote Monitoring and Management Software.
Valid Accounts	T1078	Threat actors may exploit vulnerable versions of remote access software or use legitimate, compromised credentials.
Trusted Relationship	T1199	Threat actors may leverage third party relationships to gain initial access to intended victims.

EXECUTION		
Technique Title	ID	Use
Command and Scripting Interpreter: PowerShell	T1059.001	Threat actors may use PowerShell to silently deploy remote access software. Industry has observed PowerShell being used to install RMM itself.
DEFENSE EVASION		
Technique Title	ID	Use
Masquerading	T1036	Industry has observed cyber threat actors renaming a NetSupport binary to ctfmon.exe.[2]
DISCOVERY		
Technique Title	ID	Use
Remote System Discovery	T1018	Remote access software may allow threat actors to find lists of other systems on a network that may be used for lateral movement from the current system.
LATERAL MOVEMENT		
Technique Title	ID	Use
Remote Service Session Hijacking	T1563	Threat actors may exploit existing remote services to move laterally throughout a network.
Remote Services	T1021	Threat actors may exploit valid accounts to log into a network or service designed to accept remote connections.
Exploitation of Remote Services	T1210	Threat actors may exploit remote services to gain unauthorized access to internal systems to move laterally throughout a network.
COMMAND AND CONTROL		
Technique Title	ID	Use
Remote Access Software	T1219	Threat actors may establish command and control channels using legitimate remote access software.

DETECTION

Network administrators and defenders should first establish a security baseline of normal network activity; in other words, it is critical for network defenders to be thoroughly familiar with a software's baseline behavior in order to recognize abnormal behavior and detect anomalous and malicious use. Network defenders should correlate detected activity with other suspicious behavior to reduce false positives.

The authoring agencies recommend that organizations monitor for unauthorized use of remote access software using EDR tools. Remote access software that may be leveraged by cyber threat actors includes, among others, the following:

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

REPORTING

U.S. organizations: To report suspicious or criminal activity related to information found in this joint guidance, contact your local FBI field office at fbi.gov/contact-us/field-offices or report the incident to the FBI Internet Crime Complaint Center (IC3) at ic3.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at Report@cisa.dhs.gov. For NSA cybersecurity report feedback, contact CybersecurityReports@nsa.gov. SLTT organizations should report incidents to MS-ISAC (866-787-4722 or SOC@cisecurity.org).

Israeli organizations: Contact the CERT-IL center hotline for cyber incident handling by calling "119," 24 hours a day, or via e-mail at 119@cyber.gov.il, or via encrypted e-mail download pgp key. To contact the International Operative Liaison for CERT-to-CERT engagement, email International@cyber.gov.il.

RECOMMENDATIONS FOR ALL ORGANIZATIONS

The authoring agencies recommend that organizations, specifically MSPs who leverage this software to conduct regular business, implement the mitigations below to defend against malicious use of remote access software. **Note**: These mitigations align with the Cross-Sector Cybersecurity Performance Goals (CPGs) developed by CISA and the National Institute of Standards and Technology (NIST). The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on existing cybersecurity frameworks and guidance to protect against the most common and impactful threats, tactics, techniques, and procedures. Visit CISA's Cross-Sector Cybersecurity Performance Goals for more information on the CPGs, including additional recommended baseline protections. For additional information, see the related joint Cybersecurity Advisory, Protecting Against Malicious Use of Remote Monitoring and Management Software.

ARCHITECTURE, ACCOUNTS, AND POLICY RECOMMENDATIONS

- Maintain a robust risk management strategy based on common standards, such as the National

Institute of Standards and Technology Cybersecurity Framework.

- When possible, employ zero trust solutions—or least-privilege-use configuration—which can be endpoint- or identity-based.
- Implement a user training program and phishing exercises to raise users' awareness of the risks of visiting suspicious websites, clicking on suspicious links, and opening suspicious attachments [CPG 2 .I].

  See CISA's Enhance Email & Web Security.
- Work with a security operations center (SOC) team that can assist with monitoring systems [CPG 1 .B].
- Audit Active Directory for inactive and obsolete accounts or misconfigurations.
- Enable just-in-time access and/or two-factor authentication based on the level of risks.
- Use safeguards for mass scripting and a script approval process. For example, if an account attempts to push commands to 10 or more devices within an hour, retrigger security protocols, such as multifactor authentication (MFA), to ensure the source is legitimate [3]
- Use a software bill of materials (SBOM) to maintain an inventory of components within a software product. For more information on SBOM, see CISA's Software Bill of Materials (SBOM) | CISA.
- Leverage external attack surface management (EASM) to enhance visibility across systems and infrastructures. EASM provides continuous monitoring to determine unknown assets, provide information about systems, and aid in compliance by identifying non-compliant technology, missing legal disclaimers, and expired copyright notices.

HOST-BASED CONTROLS

- Audit remote access software and their configurations on devices on your network to identify currently used and/or authorized RMM software [CPG 1 .A].
- Use security software to detect instances of RMM software only being loaded in memory.
- Review logs with complete data, including executing binary, request types, IP addresses, and date/ time, for execution of remote access software to detect abnormal use of programs running as a portable executable [CPG 2 .T].
- Implement application controls, including zero-trust principles and segmentation, to manage and control execution of software, including allowlisting RMM programs and limiting actions the software can take [CPG 2 .Q].
- Establish a regular frequency for patching, prioritizing software and systems that directly access or are accessed from the Internet, including remote access and management servers and agents.

NETWORK-BASED CONTROLS

- Implement network segmentation to minimize lateral movement and restrict access to devices, data, and applications [CPG 2 .F].

  See CISA's Layering Network Security Through Segmentation.
- Block both inbound and outbound connections on common RMM ports and protocols at the network perimeter and enforce only legitimate use of the tools employing those ports. Remote access software should have local instances in the environment and avoid operating over HTTPS port 443.
- Require authorized RMM solutions only be used from within your network over approved remote access

solutions, such as VPNs or virtual desktop interfaces (VDIs) [CPG 2 .F].

- Enable a web application firewall (WAF) to protect remote access software by filtering and monitoring HTTP traffic [CPG 2 .K].

  While this mitigation is valuable, the authoring agencies recommend IT administrators test before deploying in a production environment, WAFs have been known to disrupt normal operation of remote access tools.

RECOMMENDATIONS FOR MSP AND SAAS CUSTOMERS

The authoring agencies recommend MSP and SaaS customers:

- Ensure that they have a thorough understanding of the security services their administrators are providing via the contractual arrangement and address any security requirements that fall outside the scope of the contract. Note: Contracts should detail how and when MSPs and other providers notify the customer of an incident affecting the customer's environment.
- Enable effective monitoring and logging of their systems. If customers choose to engage an MSP or SaaS provider to perform monitoring and logging, they should ensure that their contractual arrangements require their providers to [CPGs 1 .I, 1 .G, 1 .H]:

  Implement comprehensive security event management that enables appropriate monitoring and logging of provider-managed customer systems.

  Provide visibility—as specified in the contractual arrangement—to customers of logging activities, including provider's presence, activities, and connections to the customer networks Note: Customers should ensure that MSP accounts are properly monitored and audited.
- Notify MSP of confirmed or suspected security events and incidents occurring on the provider's infrastructure and administrative networks and send these to a SOC for analysis and triage.
- Keep direct access to log servers—and the ability to delete or alter logs—out of reach of RMM tools.

RECOMMENDATIONS FOR MSPS AND IT ADMINISTRATORS

MSPs and other IT administrators provide services that usually require both trusted network connectivity and privileged access—or special access beyond that of a standard user-- to and from customer systems. Many organizations—ranging from large critical infrastructure organizations to small- and mid-sized businesses—use MSPs to manage information and communications technology (ICT) systems, store data, or support sensitive processes. Many organizations make use of MSPs to scale and support network environments and processes without expanding their internal staff or having to develop the capabilities internally.

Recommended mitigations for initial compromise attack methods include:

- Improving the security of vulnerable devices and hardening appliances to vendor best practices. For more information, see the joint Cybersecurity Information Sheet Selecting and Hardening Remote Access VPN Solutions.
- Adopting of MFA across all customer services and products [CPG 2 .H]. Note: MSPs should also implement MFA on all accounts that have access to customer environments and should treat those accounts as privileged.
- Configuring "reduced privilege" RMM tools for common uses, like read-only monitoring.

- Managing internal architecture risks and segregating internal networks [CPG 2.F].
- While zero trust is the ultimate goal, segregating customer data sets (and services, where applicable) from each other—as well as from internal company networks—can limit the impact of a single vector of attack [CPG 2.F].

    Do not reuse admin credentials across multiple customers [CPG 2.E, 2.C].

- Avoid using end-of-life (EOL) software.

Additionally, when negotiating the terms of a contract with customers, providers should give clear explanations of the services the customer is purchasing, services the customer is not purchasing, and all contingencies for incident response and recovery [CPG 1.G, 1.H].

RECOMMENDATIONS FOR DEVELOPERS OF PRODUCTS WITH REMOTE ACCESS CAPABILITIES

The authors recommend providers ensure their products:

- Include lower privilege versions and avoid executive/administrative privileges. For example, develop read-only monitoring capabilities where certain accounts can only view information from a system, but cannot implement changes to a system.
- Monitor their software and terms of service violations by cyber threat actors engaging in computer network intrusions; in particular, free trial versions are often abused by cybercriminal threat actors.
- Provide audits and logs that are difficult to delete and remove.

Additionally, the authoring agencies recommend developers:

- Incorporate threat modeling into their development processes to identify potential vulnerabilities. During development, promote fuzzing of command-line interface (CLI) commands and open network interfaces to detect vulnerabilities.
- Map practices to the Secure Software Development Framework (SSDF), which can assist in aligning products with sound and secure fundamentals, and in turn, help reduce potential vulnerabilities as well as the possible impact of undetected exploitation.
- Use advanced monitoring and incident response capabilities, which help to operationalize OT/ ICS threat detection and response for cybersecurity teams lacking expertise/infrastructure or budget to deploy full on-prem OT-specific cyber threat monitoring and management programs.

For more information for developers and manufacturers on building security principles into their products, see the joint guidance Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security- by-Design and -Default.

DISCLAIMER

The information in this report is being provided "as is" for informational purposes only. CISA, NSA, FBI, MS-ISAC, and INCD do not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial entities or commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoritism by CISA, NSA, FBI, MS-ISAC, and INCD.

ACKNOWLEDGEMENTS

CNWR, ConnectWise, Corporate Information Technologies, Google, Honeywell, Huntress, (ISC)² Inc., N-Able, Tenable, and VMware contributed to this guidance.

RESOURCES

- CISA's Cross-Sector Cybersecurity Performance Goals
- CISA Strategic Plan 2023-2025
- Protecting Against Malicious Use of Remote Monitoring and Management Software | CISA
- Joint CSA Protecting Against Cyber Threats to Managed Service Providers and their Customers
- CISA Insights Mitigations and Hardening Guidance for MSPs and Small- and Mid-sized Businesses
- Protecting Against Cyber Threats to Managed Service Providers and their Customers | CISA
- Joint Guidance Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default
- People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection
- What is RMM (connectwise.com)
- What Is Remote Monitoring and Management (RMM)? (intel.com)
- Remote monitoring and management abuse - Threat Detection Report (redcanary.com)

REFERENCES

[1] https://www.ninjaone.com/blog/what-is-remote-access-software-guide-2023/

[2] Remote access tool or trojan? How to detect misbehaving RATs (redcanary.com)

[3] https://level.io/blog/how-to-secure-rmms