MANDIANT
NOW PART OF Google Cloud

Remediation + Hardening Guide

ConnectWise ScreenConnect

CVE-2024-1708 & CVE-2024-1709

v1.0

Summary

This document contains remediation and hardening recommendations for responding to critical vulnerabilites for the ConnectWise ScreenConnect application announced on February 19, 2024.

- CVE-2024-1708
- CVE-2024-1709

The original advisory from ConnectWise can be found here.

Remediation Summary:

- If you have a cloud based controller, no action is required as ConnectWise has applied the necessary patches.
- If you have on-premises servers hosting the ScreenConnect application, review this guide for suggested actions.

Created: February 23, 2024
Updated: February 23, 2024

Change Log

Version	Date	Updates
1.0	Feb 23, 2024	Initial Document

Table of Contents

Background

On February 19, 2024, ConnectWise announced two (2) CVEs for their ScreenConnect product affecting (on-premises) versions 23.9.7 and earlier.

- CVE-2024-1708 - Authentication Bypass Vulnerability (10.0)
- CVE-2024-1709 - Path Traversal Vulnerability (8.4)

These vulnerabilities allow an unauthenticated actor to bypass authentication and access ScreenConnect environments that may be behind a corporate firewall.

ConnectWise has released updated versions of the ScreenConnect product (23.9.8+) that mitigate the vulnerabilities. ConnectWise has removed license restrictions so ScreenConnect consumers who no longer have a maintenance subscription can update their software.

Proactive Preparation and Hardening Actions

Mandiant recommends all ConnectWise ScreenConnect customers execute the following steps, even if they currently have not identified evidence of compromise.

- **Update ScreenConnect to the latest version.** Immediately update ScreenConnect to version 23.9.8 (or higher) to protect against exploitation of the reported vulnerabilities.

- **Baseline activities in the audit log.** Leverage the ScreenConnect audit log and triggers to generate a baseline of interactions issued to endpoints. Mandiant recommends the following actions be included for auditing to help identify suspicious activity or potential evidence of compromise.

  - `QueuedTool`
  - `QueuedInstallAccess`
  - `ProcessedTool`
  - `RanCommand`
  - `SentFiles`
  - `QueuedElevatedTool`
  - `QueuedCommand`
  - `ProcessedCommand`
  - `ModifiedIsPublic`
  - `ModifiedHost`
  - `CopiedFiles`
  - `RanFiles`

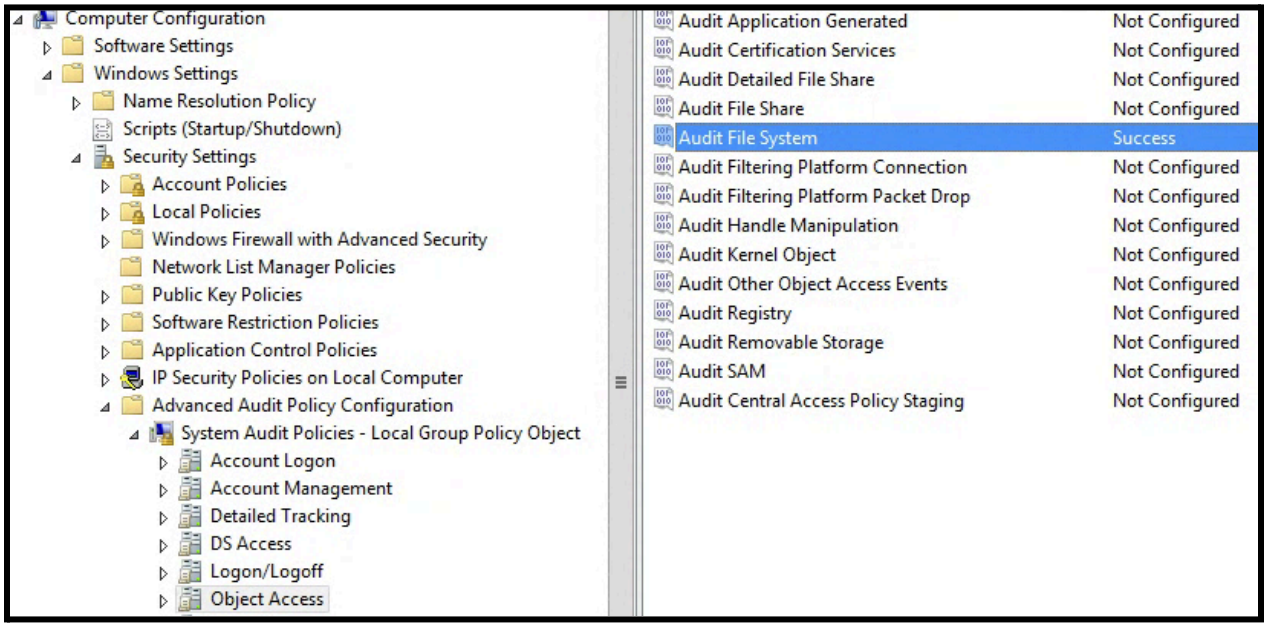
  For additional information, reference:
  - https://docs.connectwise.com/ConnectWise_ScreenConnect_Documentation/Get_started/Administration_page/Triggers_page/List_of_trigger_definitions
  - https://docs.connectwise.com/ConnectWise_ScreenConnect_Documentation/Get_started/Administration_page/Audit_page/Generate_a_basic_audit_report

- **Enable Advanced Audit Policy Logging.** To capture file access and write events (Event ID 4663) that may be indicative of compromise, on the servers hosting the ScreenConnect application, enable Windows Advanced Audit Policy logging for the following default directories:
  - `C:\Windows\Temp\ScreenConnect\<version>\`
  - `C:\Program Files *\ScreenConnect\App_Extensions\`

  When collected and forwarded to a SIEM, these events can be used to help correlate malicious activity with other forensic artifacts.

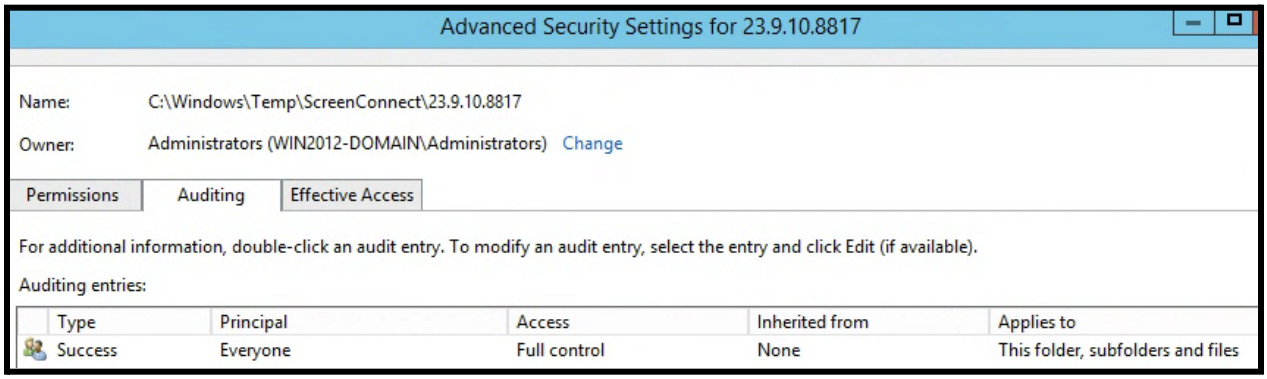
  Advanced Audit Policy logging in Windows can be configured using either local or group policy settings:

- `Computer Configuration > Windows Settings > Security Settings > Advanced Audit Policy Configuration > System Audit Policies > Object Access > Audit File System`
    - `Success`



Once enabled, navigate to the specific folders required for monitoring and define the types of accesses that should be audited and recorded.

- Right click the `folder > Properties > Security > Advanced > Auditing` tab
    - Click `Add > Select a Principal` (e.g., `Everyone`)
        - Click `Show Advanced Permissions`
            - Select the appropriate permissions that should be recorded



Note: Enabling Advanced audit policy logging can cause operational impacts on high transaction servers. It is only recommended to configure and enforce the recommendations for a specific set of folders or files required for monitoring.

- **Review and Baseline ConnectWise Extensions.** Inventory and review any extensions installed for the ScreenConnect application. For additional information, reference: https://docs.connectwise.com/ConnectWise_ScreenConnect_Documentation/Get_started/Administration_page/Extensions_page

- **Log and Forward Inbound Web Requests.** Exploitation of CVE-2024-1709 relies on submitting a web request for the `SetupWizard.aspx` file and providing additional parameters within the request (e.g. `SetupWizard.aspx/additionalcontent`).

  Ensure that firewalls or load balancers that are placed in front of ScreenConnect server(s) are able to capture and log inbound web requests. Additionally, organizations should ensure that logs capturing inbound web requests are forwarded to a centralized SIEM, where alerting and detections can be configured for abnormal requests that include the `SetupWizard.aspx` file.

- **Enable X-Forwarded-For Request Header Logging.** If a load balancer or reverse proxy server is placed in front of ScreenConnect server(s), ensure that the `X-Forwarded-For` field is enabled to capture the true external IP address associated with inbound requests.

- **Disable Access to the SetupWizard file.** As a temporary hardening action, consider editing or removing access to the `C:\Program Files*\ScreenConnect\SetupWizard.aspx` file so that it cannot execute if ScreenConnect is already configured.

- **Restrict egress connectivity from ConnectWise servers.** Egress communications for the server(s) hosting the ConnectWise application(s) should follow a deny-list approach using a Layer 7 firewall or network filtering appliance.. This strategy can prevent potential backdoors or reverse shells from establishing egress connectivity to command and control infrastructure.

Containment and Initial Investigative Steps

Mandiant recommends organizations that are running impacted versions of the ConnectWise ScreenConnect application follow the processes outlined below for immediate containment and investigative actions.

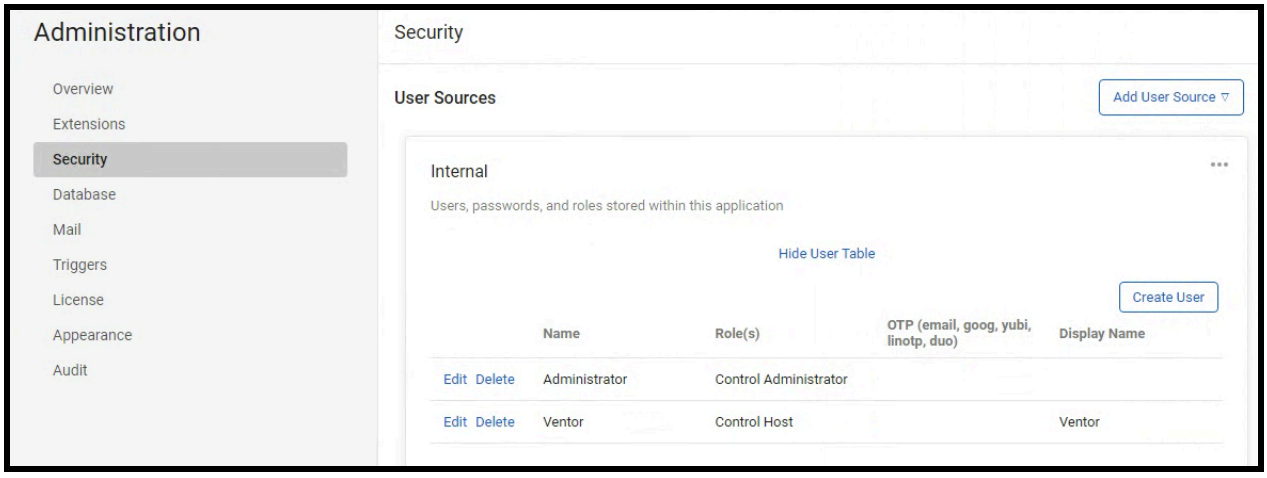
- **Isolate and Preserve impacted server(s).** Immediately isolate any servers running the ScreenConnect application and preserve the current state image(s) in order to perform a comprehensive forensic review and investigation. The server(s) should ***not*** be placed back into production until they are rebuilt, patched, and a comprehensive investigation has been conducted.

  If a full system image cannot be preserved, at a minimum, preserve files located within the `C:\Program Files*\ScreenConnect\App_Data\` directory.

- **Hunt for Indicators.** ConnectWise has published IOCs for known attempts to exploit the identified vulnerabilities. As part of post-exploitation, Mandiant has identified lateral movement from vulnerable ScreenConnect servers to additional systems within client environments (including Domain Controllers). The scope of an investigation should include more than just the vulnerable ScreenConnect server(s).

- **Query the ScreenConnect Audit Log.** Leverage the ScreenConnect audit report / triggers to review interactions issued to endpoints. ConnectWise has published available Session Event types here. Specific event types of interest could include:
  - `QueuedTool`
  - `QueuedInstallAccess`
  - `ProcessedTool`
  - `RanCommand`
  - `SentFiles`
  - `QueuedElevatedTool`
  - `QueuedCommand`
  - `ProcessedCommand`
  - `ModifiedIsPublic`
  - `ModifiedHost`
  - `CopiedFiles`
  - `RanFiles`

- **Hunt for suspicious users added to the ScreenConnect application.** The default security database for the ScreenConnect application (`Security.db)`is stored within the `C:\Program Files*\ScreenConnect\App_Data\` directory. Review the user table for newly added or suspicious accounts.
  Note: The listing of locally configured ScreenConnect users is also available within the `Administration > Security > User Sources` page.



- **Search for Unexpected ScreenConnect Extensions.** ScreenConnect allows for customers to extend the capabilities of the product by installing extensions. Review the listing of installed extensions to ensure that malicious or unauthorized extensions have not been added. Per the Huntress report, any `aspx` or ashx files residing in the `C:\Program Files*\ScreenConnect\App_Extensions\` directory may be indicative of exploitation of CVE-2024-1708.

- **Hunt for Suspicious Commands.** ScreenConnect allows for commands to be executed on remote machines where agents are installed. Remote commands can include invocation of executables, Windows command shell activity, or PowerShell. Leverage available PowerShell logging and Windows Event Process logging to look for abnormal commands and scripts that may have been executed.

- **Hunt for ConnectWise Command Artifacts.** Examine endpoint process starts for PowerShell or CMD execution with command line arguments referencing `.PS1` files or `.CMD` files within the `C:\Windows\Temp\ScreenConnect\<Version>\` directory. Additionally, look for suspicious processes executed with `ScreenConnect.ClientService.exe` as the parent process.

- **Hunt for Suspicious use of BITSADMIN.EXE.** Investigate any instance where PowerShell or `cmd.exe` invoked `BITSADMIN` on endpoints.

- **Examine web / firewall logs for suspicious requests.** Exploitation of CVE-2024-1709 relies on submitting a web request for the `SetupWizard.aspx` file and providing additional parameters within the request (e.g., `SetupWizard.aspx/additionalcontent`). Review available firewall logs for requests to `SetupWizard.aspx` that include additional parameters (`SetupWizard.aspx/` or `SetupWizard.aspx/*`).

The source IP address(es) and login status for requests can also be reviewed within the ScreenConnect Audit log (`Admin > Audit` page).

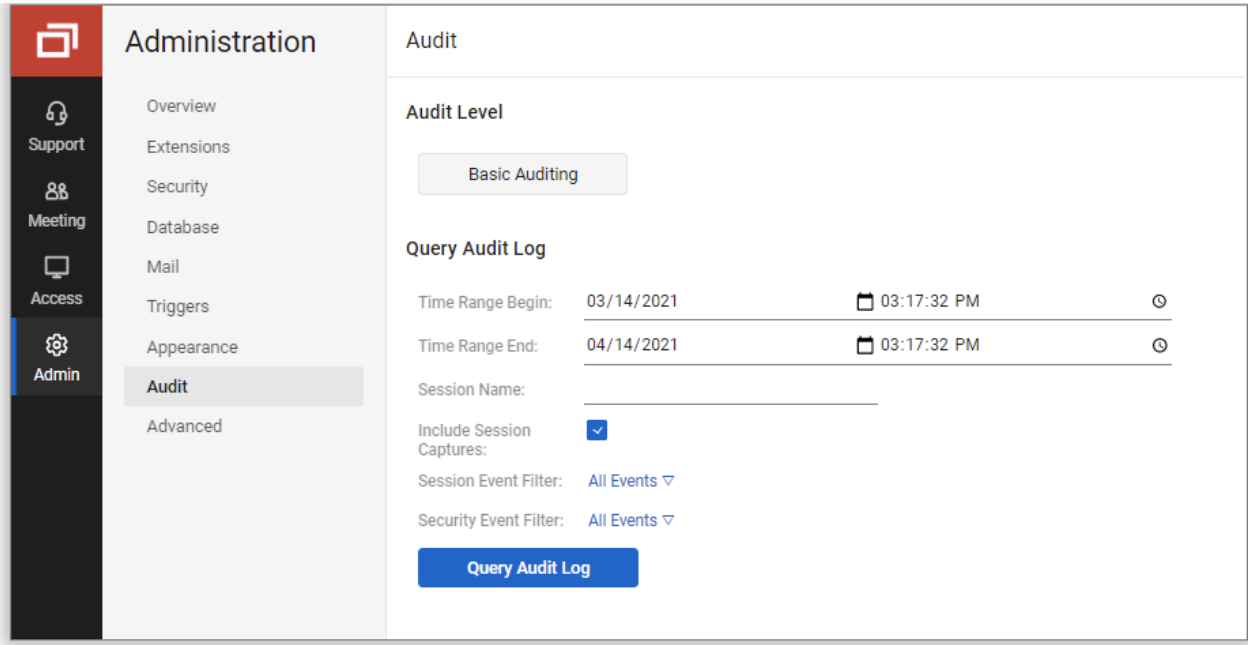


Image Source:
https://docs.connectwise.com/ConnectWise_ScreenConnect_Documentation/Get_started/Administration_page/Audit_page/Generate_a_basic_audit_report

Remediation Steps

Mandiant recommends organizations that are running impacted versions of the ConnectWise ScreenConnect application follow the steps below for remediation actions.

- **Rebuild / Patch.** As of February 22, 2024, Mandiant has identified extensive automated exploitation of the identified vulnerabilities. These exploitation attempts have resulted in persistence on the ScreenConnect servers using methods such as:
    - Creating net new privileged users within the ScreenConnect application and on the server(s) hosting the application(s).
    - Implanting web shells and backdoors
    - Downloading and staging additional tools for lateral movement and remote access

  Based upon these observances, Mandiant recommends ***rebuilding*** impacted servers running the ScreenConnect application before placing it back into production. This would include rebuilding the ScreenConnect servers using trusted operating systems builds and re-installing the application using the latest (patched) version (23.9.8+).

- **Creating net new accounts for the ScreenConnect application.** Create net-new accounts for the ScreenConnect application and on the local server(s) hosting the application.

- **Reset password(s) for local administrator accounts** on the server(s) - especially if these accounts share a common password with other accounts in the environment.

- **If an external database is used for ScreenConnect,** rotate accounts associated with the database services.

- If the investigation identifies lateral movement, **Perform an Enterprise Password Reset** (EPR) to systems that house potentially exposed / impacted credentials (e.g., Active Directory).

Additional Hardening Measures

If lateral movement has been identified within an on-premises Active Directory environment, additional containment, remediation, and hardening measures may be required.

Identify and Reduce the Scope of Privileged Accounts in Active Directory
MITRE ATT&CK ID: T1078

To reduce the attack surface of an on-premises Active Directory (AD) environment, organizations should proactively identify and attempt to reduce the scope of accounts that are provided privileged access. Specifically, any Active Directory integrated accounts that can directly interface with ScreenConnect servers should not be granted permissions to administer Tier 0 servers / endpoints and applications.

The following built-in Active Directory groups represent a significant level of privileged groups within AD, and are often targeted by threat actors for privilege escalation, lateral movement, and persistence.

- `Domain Admins`
- `Enterprise Admins`
- `Schema Admins`
- `Administrators`
- `Account Operators`
- `Backup Operators`
- `Cert Publishers`
- `Print Operators`
- `Server Operators`
- `DNS Admins`
- `Replicator`
- `Group Policy Creator Owners`
- `Denied RODC Password Replication Group`
- `Distributed COM Users`

Using the Active Directory PowerShell cmdlet module, group membership for the aforementioned groups can be enumerated. An example is provided below:

```
Unset
get-ADGroupMember -Identity "Domain Admins" -Recursive | export-csv -path <path to csv export>
```

Note: If an organization leverages virtualized infrastructure (on-premises or cloud) to host applications and services, any accounts that provide administrative access to the platforms should also be considered as a "privileged" role. The scope of accounts that are provided this level of

access should be reviewed and minimized, in addition to the enforcement of security controls that restrict administrative access to only specific IP addresses / subnets associated with privileged identities.

Reduce the Scope of Permissions Assigned to Privileged Accounts

To inhibit a threat actor's ability to leverage a compromised system or credential to escalate privileges and laterally move within an environment, organizations should review the operational necessity for any accounts that have elevated permissions on endpoints, and work to reduce the scope of privileges assigned to users and services.

Standard user accounts should not require administrative privileges to perform daily job functions and services should operate with the lowest privilege level possible.

Tiered Accounts

All personnel that are assigned administrative responsibilities should utilize separate accounts for administrative functions - that are distinct from normal user accounts.

- **Standard user accounts:** Granted standard user privileges for common user tasks - such as email, web browsing, and using various corporate applications. These accounts should not be granted administrative privileges on endpoints.
- **Administrative (secondary) accounts:** Separate accounts created for personnel who are assigned various tiers of administrative privileges. An administrator who is required to manage assets in each Tier (discussed below) should utilize a separate account for each Tier. These accounts should not be leveraged to access email or used for web browsing - and should be explicitly restricted to only be leveraged within each Tier.

For secondary accounts that have privileged access (i.e., Enterprise Admin, Domain Admin, Exchange Admin) throughout the environment, these accounts should not be utilized on standard workstations and laptops, but from designated systems (ex: jump boxes) that reside in restricted and protected VLANs and Tiers. Consider blocking any accounts with enterprise and/or domain administrative access from being able to login (remotely or locally) to standard workstations, laptops, and common access servers.

For the group policy object (GPO) settings referenced below, the settings are configurable via the path of:

```
Unset
Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment
```

Accounts delegated with local or domain privileged access should be explicitly denied access to standard workstations and laptops systems within the context of the following settings (which can be configured using a GPO):

- `Deny access to this computer from the network (SeDenyNetworkLogonRight)`
- `Deny log on as a batch job (SeDenyBatchLogonRight)`
- `Deny log on as a service (SeDenyServiceLogonRight)`
- `Deny log on locally (SeDenyInteractiveLogonRight)`
- `Deny log on through Terminal Services (SeDenyRemoteInteractiveLogonRight)`
- `Debug programs (SeDebugPrivilege) - should be removed for all users - including local administrators`

In addition, organizations should consider designing and staging protected tiered network segments within the environment - and designate these segments as the only authorized origination point from which privileged functions can occur (e.g., remote server administration, database management, application management, Active Directory management, help desk functions). This should be enforced by controls at the network, Active Directory, and endpoint-based layers.

Ideally, the architecture should support various Tiers for access control:

- Tier 0 = Domain Controllers and highly critical services
- Tier 1 = Servers and Hosted Applications
- Tier 2 = User Workstations, Laptops, and common access servers

Additional security controls for consideration:

- Direct access (using administrative and management ports) from Tier 2 systems to Tier 0 systems should be explicitly blocked.
- Specific accounts should only be delegated access to Tier 0 systems (and only initiated from systems within the Tier 0 layer).
- Specific accounts should only be delegated access to Tier 1 systems (and only initiated from systems within the Tier 1 layer).

On Tier 2 systems, accounts delegated for Tier 0 and Tier 1 access should be explicitly denied for access using the following settings (which can be configured within the context of GPO settings):

- `Deny access to this computer from the network (also include S-1-5-114: NT AUTHORITY\Local account and member of Administrators group)`
- `Deny log on as a batch job`
- `Deny log on as a service`
- `Deny log on locally`

- `Deny log on through Terminal Services (also include S-1-5-114: NT AUTHORITY\Local account and member of Administrators group)`

On Tier 1 systems, accounts delegated for Tier 0 access should be explicitly denied access – using the following settings (which can be configured within the context of GPO settings):

- `Deny access to this computer from the network`
- `Deny log on as a batch job`
- `Deny log on as a service`
- `Deny log on locally`
- `Deny log on through Terminal Services`

On Tier 0 systems, only accounts designated for Tier 0 administration purposes should be granted access - using the following settings (which can be configured within the context of GPO settings):

- `Allow log on locally`
- `Allow log on through Terminal Services`

Lateral Movement Tactics and Associated Hardening Controls

The table below contains common tactics and the associated hardening controls that can be leveraged to combat remote access tools and methods from being utilized for lateral movement within an environment.

Tool / Tactic	Mitigating Endpoint Security Configuration(s)

MITRE ATT&CK ID: T1021.002
 	
PSExec (using the current logged-on user account, without the -u switch)
 	
If the -u switch is not leveraged, authentication will use Kerberos or NTLM for the current logged-on user of the source endpoint – and will register as a Type 3 (network) logon on the destination endpoint.
 	
PSExec – high level functionality:
 	
• Connects to the hidden ADMIN$ share (mapping to the C:\Windows folder) on a remote endpoint via SMB (TCP/445).
 	
• Utilizes the Service Control Manager (SCM) to start the PsExecsvc service and enable a named pipe on a remote endpoint.
 	
• Input/output redirection for the console is achieved via the created named pipe.
	(Mitigating options are listed from least to most impactful to business operations, and should be carefully tested prior to full deployment)
	
	Option 1: GPO Configuration
	
	`Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment`
	• `Deny access to this computer from the network`
	
	Option 2: Windows Firewall Rule enforcement on endpoints
	
	Unset
	`netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=no`
	
	Option 3: Disable administrative and hidden shares on endpoints using a GPO.
	
	`Computer Configuration > Policies > Administrative Templates > MSS (Legacy) > MSS (AutoShareServer)`
	• `Disabled`
	`Computer Configuration > Policies > Administrative Templates > MSS (Legacy) > MSS (AutoShareWks)`
	• `Disabled`

MITRE ATT&CK ID: T1021.002 PSExec (with Alternative Credentials, via the -u switch)	**Option 1: GPO Configuration** `Computer Configuration > Policies > Windows Settings > Security Settings >`

Tool / Tactic	Mitigating Endpoint Security Configuration(s)

If the -u switch is leveraged, authentication will use the alternate supplied credentials – and will register as a Type 3 (network) and Type 2 (interactive) logon on the destination endpoint.	`Local Policies > User Rights Assignment`
	• `Deny access to this computer from the network`
	• `Deny log on locally`
	
	Option 2: Windows Firewall Rule enforcement on endpoints
	
	Unset
	`netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=no`

MITRE ATT&CK ID: T1021.001
 	
Remote Desktop Protocol (RDP)
	Option 1: GPO Configuration
	
	`Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment`
	• `Deny log on through Terminal Services`
	
	Option 2: Windows Firewall Rule enforcement on endpoints
	
	Unset
	`netsh advfirewall firewall set rule group="Remote Desktop" new enable=no`

MITRE ATT&CK ID: T1021.006
 	
PS Remoting and WinRM
	Option 1: PowerShell Command
	
	Unset
	`Disable-PSRemoting -Force`
	
	Option 2: GPO Configuration
	
	`Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Remote Management`

Tool / Tactic	Mitigating Endpoint Security Configuration(s)
	(WinRM) > WinRM Service > Allow remote server management through WinRM • Disabled **Option 3: Windows Firewall Rule enforcement on endpoints** ``` Unset netsh advfirewall firewall set rule group="Windows Remote Management" new enable=no ```
MITRE ATT&CK ID: T1021.003 Distributed Component Object Model (DCOM)	**Option 1: GPO Configuration** Computer Configuration > Policies > Windows Settings > Local Policies > Security Options • DCOM:Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) Syntax Computer Configuration > Policies > Windows Settings > Local Policies > Security Options • DCOM:Machine Access Restrictions in Security Descriptor Definition Language (SDDL) Syntax Both settings allow an organization to define additional computer-wide controls that govern access to all DCOM–based applications on an endpoint. When users or groups that are to be given permission are specified, the security descriptor field is populated with the SDDL representation of those groups and privileges. Users and groups can be given explicit Allow or Deny privileges on both local access and remote access. **Option 2: Windows Firewall Rule enforcement on endpoints (one rule specific to DCOM):**

Tool / Tactic	Mitigating Endpoint Security Configuration(s)

	Unset
	`netsh advfirewall firewall set rule name="DFS Management (DCOM-In)" new enable=yes`
	
	`netsh advfirewall firewall set rule group="DFS Management" new enable=yes`
	
	(four rules In total should be generated from the above commands)

MITRE ATT&CK IDs: T1563 / T1570 Third-Party Remote Access Applications (e.g., VNC / DameWare / ScreenConnect / AnyConnect)	**Option 1: GPO Configuration** `Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment` • `Deny access to this computer from the network` • `Deny log on locally`