MANDIANT
NOW PART OF Google Cloud

MOVEit Transfer: Containment and Hardening Guide

V1.7 – JULY 06, 2023

Change Log

Version / Date	Notes
1.0: June 01, 2023	Initial Document
1.1: June 02, 2023	Minor updates / edits throughout document
1.2: June 06, 2023	Added a containment recommendation for clearing active sessions Added a subtask "Review database logs for file download events" within the "Logging and Hunting Recommendations" section
1.3: June 07, 2023	Updated Overview section to include references to the assigned CVE-2023-34362 Added information about risks of credential stuffing attacks for local accounts Added information about package archives – and potential risks related to data exposure / theft.
1.4: June 09, 2023	Updates throughout the document to include references to newly identified vulnerabilities (disclosed as of June 9, 2023). Updated the "Review IIS Logging Settings" section to provide additional clarity, configuration options, and detections.
1.5: June 12, 2023	Updated multiple sections to reference CVE-2023-35036 (newly assigned CVE for the June 9, 2023 disclosed vulnerabilities).
1.6: June 17, 2023	Updated multiple sections to reference CVE-2023-35708. Added a new subsection (Restrict Inbound Traffic) within the "Application and Infrastructure Hardening Recommendations" section.
1.7: July 06, 2023	Updates throughout the document to include references to newly identified vulnerabilities (CVE-2023-36934, CVE-2023-36932, CVE-2023-36933) and associated patches / service packs (disclosed as of July 5, 2023).

Contents

MOVEit Transfer: Containment and Hardening Guide

This is a work-in progress document – and will be updated as new information for hardening and mitigations are identified.

MOVEit Transfer – Critical Vulnerability Overview

On May 31, 2023, Progress Software (Progress) discovered a vulnerability in the MOVEit Transfer application that could lead to escalated privileges and potential unauthorized access within an environment where the application is deployed. The MOVEit Transfer application is a file transfer solution that allows for secure file transfers using either HTTPs, SCP, or FTPs. On June 2, 2023, CVE-2023-34362 was assigned for the associated SQL injection vulnerability.

On June 9, 2023, cybersecurity firm Huntress (working with Progress) uncovered additional vulnerabilities (tracked as CVE-2023-35036) that could potentially be leveraged for exploitation of the MOVEit Transfer application. Additional patches were released - and are recommended to be applied to all MOVEit Transfer instances.

On June 15, 2023, Progress disclosed an additional vulnerability (CVE-2023-35708) impacting the MOVEit Transfer application that could lead to escalated privileges and potential unauthorized access to an environment. Subsequent patches to mitigate CVE-2023-35708 were released on June 16, 2023.

On July 5, 2023, Progress announced the formalization of scheduled Service Pack updates for MOVEit products. With the release of the July 2023 Service Pack updates, Progress announced additional vulnerabilities (CVE-2023-36934, CVE-2023-36932, and CVE-2023-36933) impacting specific MOVEit Transfer versions.

Table 1 provides an overview of the impacted software versions, and the corresponding patched versions (as of July 5, 2023) that Progress indicates mitigate the six (6) identified CVEs:

- CVE-2023-34362
- CVE-2023-35036
- CVE-2023-35708
- CVE-2023-36934
- CVE-2023-36932
- CVE-2023-36933

Impacted Version	Patched Version
MOVEit Transfer 2023.0.0	MOVEit Transfer 2023.0.4
MOVEit Transfer 2022.1.x	MOVEit Transfer 2022.1.8
MOVEit Transfer 2022.0.x	MOVEit Transfer 2022.0.7
MOVEit Transfer 2021.1.x	MOVEit Transfer 2021.1.7
MOVEit Transfer 2021.0.x	MOVEit Transfer 2021.0.9
MOVEit Transfer 2020.1.x (12.1)	MOVEit Transfer 2020.1.11 (special Service Pack required)
MOVEit Transfer 2020.0.x (12.0) or older	MUST upgrade to a supported version

MOVEit Cloud	Prod: 14.1.6.97 or 14.0.5.45 Test: 15.0.2.39

Table 1: Impacted and patched software versions via https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023 and https://community.progress.com/s/article/MOVEit-Transfer-Service-Pack-July-2023

Note: If customers already applied the June 2 patches to mitigate CVE-2023-34362, a DLL drop-in method for mitigating CVE-2023-35036 and CVE-2023-35708 can be considered. Progress has provided additional information related to this upgrade process.

https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-CVE-Pending-Reserve-Status-June-9-2023

https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-15June2023

To minimize the potential impact, the following steps should be conducted immediately:

- Apply all relevant patches as recommended by Progress.
- Disable all inbound and outbound communications (e.g., HTTP and HTTPs traffic) related to the MOVEit Transfer application.
- Isolate the servers hosting the application, to perform a forensic investigation.
- Check for potential indicators of unauthorized access for at least the last 30 days, including:
    - The creation of unexpected files in the `c:\MOVEit Transfer\wwwroot\` folder on all MOVEit Transfer instances (including back-ups)
    - Unexpected and/or large file downloads

Active Exploitation Details

Mandiant has observed threat actors actively exploiting the CVE-2023-34362 vulnerability in May and June 2023. In some instances, the threat actor leveraged the vulnerability to deploy a web shell to the impacted MOVEit Transfer server. The web shell performed the following actions:

- Extracted Azure configuration details, including:
    - Azure storage account name
    - Azure storage account access keys
    - Azure blob storage container name
- Queried the connected SQL database for multiple datasets, including:
    - Listing of all files uploaded to the application, including file path, uploader name, file size, and other metadata
    - Listing of all folders including the path and folder owner
    - Listing of all organizations configured in the application
- Added all extracted data to a compressed GZIP file which was returned in a HTTP(s) response

Document Scope

This document provides additional containment and hardening steps that should be considered for environments that leverage the MOVEit Transfer application.

Containment Recommendations

Isolate Impacted Servers, Patch, and Investigate

Goals: Mitigate the risk of future exploitation of this vulnerability and keep impacted servers isolated from the rest of the environment until an investigation has been completed.

Disable Inbound and Outbound Communications to Application

Disable all inbound and outbound communications (e.g., HTTP and HTTPs traffic) related to MOVEit Transfer application. This can be accomplished by modifying rules on a network or local firewall to block TCP port 80 and 443 to and from the impacted server.

Note: Progress provided the following guidance on how this recommendation will impact the functionality of the application (source: https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023):

- It is important to note, that until HTTP and HTTPS traffic is enabled again:
  - Users will not be able to log on to the MOVEit Transfer web UI
  - MOVEit Automation tasks that use the native MOVEit Transfer host will not work
  - REST, Java and .NET APIs will not work
  - MOVEit Transfer add-in for Outlook will not work

  Please note: SFTP and FTP/s protocols will continue to work as normal
- As a workaround, administrators will still be able to access MOVEit Transfer by using a remote desktop to access the Windows machine and then accessing https://localhost/.

For more information on localhost connections, reference:

https://docs.progress.com/bundle/moveit-transfer-web-admin-help-2023/page/Security-Policies-Remote-Access_2.html

Isolate Server Hosting the Application

Consider completely isolating the server hosting the application until a forensic investigation can be conducted and patches are applied to the impacted application. This can be accomplished by placing the servers on an isolated VLAN or by using endpoint security software that provides the ability to contain an endpoint.

Patch and Update

As Progress provides patches, impacted versions of the MOVEit Transfer software should be updated.

Note: As of June 16, 2023, Progress has released patches for the impacted MOVEit Transfer application versions for which multiple vulnerabilities were identified.

To ensure that the latest patches have been applied, reference:

https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023

https://community.progress.com/s/products/moveit/product-lifecycle

Conduct an Investigation

Conduct a forensic investigation to determine if a threat actor exploited the vulnerabilities in the MOVEit Transfer application and gained unauthorized access to additional infrastructure (on-premises or cloud environments). The Logging and Hunting section contains recommendations to help organizations identify evidence of a threat actor exploiting this vulnerability and examples of post-exploit activity observed by threat actors exploiting this vulnerability in the wild.

If exploitation is suspected, conduct a comprehensive investigation, and develop a customized remediation strategy.

Rebuild / Server Reconstitution

In the event of an application compromise that resulted in backdoors, web shells, or other suspicious artifacts being present on a server, a preservation of the compromised server, followed by a clean-source server replacement to host a patched version of the MOVEit Transfer software may be required.

In the event that a server rebuild and clean-source application installation is not an option, any identified web shells (`human2.aspx`), backdoors, or suspicious accounts should be removed prior to placing the server hosting the MOVEit Transfer application back into production.

Clearing of Active Sessions

Goal: Clear active sessions to minimize the risk a threat actor regaining access to the MOVEit Transfer application.

If the MOVEit Transfer application will be restored and reconstituted using a snapshot or backup that preserved active sessions, all existing sessions should be cleared and terminated prior to placing the application back into production.

Within the Administrator home page for within the MOVEit Transfer WebUI, an administrator can view:

- The number of active sessions by interface type
- The number of unique users connected
- The total number of current sessions

Active Sessions can be accessed in the **Session Manager** component of the **Session Summary** section. This will provide a list of currently signed-in users, correlating IP addresses, interface type, and event timestamps. Sessions can be removed on a per-user or "all sessions" basis.

For additional information related to reviewing and clearing active sessions within the MOVEit Transfer application, reference:

https://community.progress.com/s/article/Admin-Features-on-the-Home-Page-in-MOVEit-Transfers-Web-Interface

Credential Rotation and Hardening

MITRE ATT&CK ID: TA0006

Goal: Rotate passwords and other secrets to revoke access from potentially exposed credentials.

Prior to reconstituting the application back into production, in addition to clearing active sessions, credential rotation should occur for accounts, secrets, and keys associated with the MOVEit Transfer application.

Credential rotation is particularly important for local accounts that are configured within the MOVE it Transfer application. If accounts local to the application (which can be stored within the backend database) are configured with the same password that can also be used to access other infrastructure or services, this elevates risks related to credential stuffing and expanded access by a threat actor.

Local Application Credentials / API Access

The web user interface (UI) provides the ability to configure local accounts (users / administrators) for the MOVEit application. Any accounts that are present within the application should have their credentials rotated.

The process for requesting passwords to be changed for MOVEit Transfer accounts is referenced below:

https://docs.progress.com/bundle/moveit-transfer-signon-help-2022/page/Perform-or-Request-a-Password-Change.html

Additionally, security questions and MFA should also be configured for accounts that use the MOVEit Transfer application. The full range of security configuration options available for the application-specific accounts are referenced below:

https://docs.ipswitch.com/MOVEit/Transfer2021/Help/Admin/en/index.htm#48287.htm

https://docs.progress.com/bundle/moveit-transfer-web-admin-help-2022/page/Multi-Factor-Authentication.html

Note: Application credentials can also be used for accessing MOVEit Transfer using the REST API (licensed feature). By default, access tokens for the API are valid for a 20 minute period.

For additional Information related to the REST API, reference:

https://community.progress.com/s/article/HTTP

https://docs.ipswitch.com/MOVEit/Transfer2020/API/rest/#section/Handling-Session-Tokens/Requestrefresh-an-access-token

Exploitation of the vulnerability may allow a threat actor to create rogue accounts within the application. Reference the Logging and Hunting Recommendations section for additional indicators related to this tactic. Administrators should review the application to identify any suspicious (newly created) accounts, or dormant accounts which can be removed.

For additional information related to account management, reference:

https://docs.progress.com/bundle/moveit-transfer-web-admin-help-2022/page/Users.html

Local Server Credentials

As the MOVEit application is installed on a Windows server, credentials for accounts that reside on the server should be rotated. Credential rotation should include not only local accounts, but also Active Directory accounts that have the ability to log on locally or remotely to the servers.

Note: As part of installation, the MOVEit application may create local administrative service accounts on a server. Both of these accounts should have the associated passwords rotated.

- `moveitsvc` (MOVEit Transfer service)
- `miadmin` (MOVEit Automation service)

The process for rotating these passwords is referenced below:

https://community.progress.com/s/article/Transfer-Automation-Change-Windows-Service-Account-Password

Domain / LDAP Credentials

If the MOVEit application is installed on a domain-joined Windows server, credentials for any accounts that have been utilized for local or remote access to the server and application should also be rotated. This could include rotating credentials from accounts associated with domain administrators, server administrators, and information technology support staff.

If accounts are synced from an external LDAP store, the `SyncLDAP.Log*` files (located in the `MOVEitTransfer\Logs\` directory) can be reviewed to identify any suspicious or unknown accounts associated with the application.

Local Data Encryption Keys

Encryption keys should be rotated, to re-encrypt the local (at-rest) filestore. The key rotation dashboard feature of the MOVEit Transfer application can allow for re-encryption to be either on-demand or based upon a pre-defined schedule.

For additional information related to local data encryption key rotation, reference:

https://docs.progress.com/bundle/moveit-transfer-web-admin-help-2022/page/Encryption-Keys.html

Azure API Keys and Credentials

If the MOVEit application is configured to leverage an Azure blob for file storage, additional configuration information is required to be present within the application (including Azure storage API keys, account name, and container name - reference Figure 1). If this configuration is present, Azure storage account access keys should be proactively rotated. An Azure storage account provides two access keys, primary and secondary. As a precaution, both access keys should be rotated, with one of the new access keys then needing to be updated in the configuration.

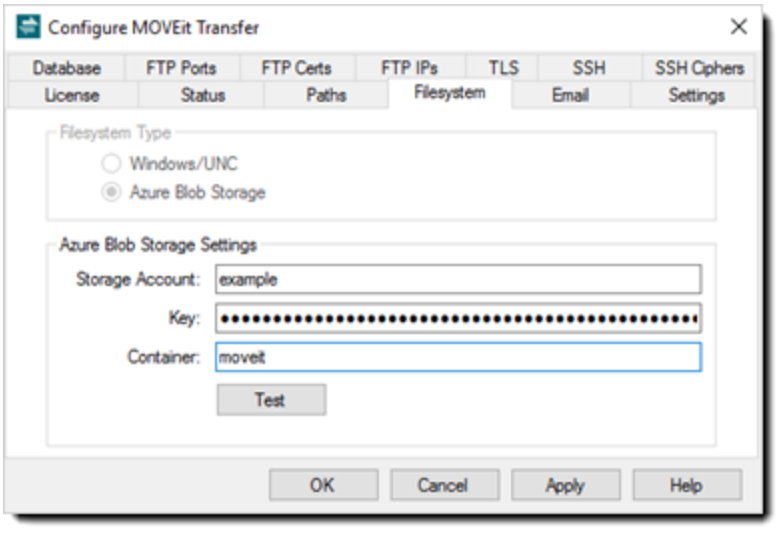

Figure 1 Azure Storage Account registration in the MOVEit Transfer Config

Azure Storage Account access keys can be rotated in the Azure management portal, via Azure CLI or Azure PowerShell.

Note: Rotating an access key makes the current access key invalid. Any systems, applications, or identities using the access key will lose access to all services available on the storage account. Additionally, SAS tokens and any links using SAS tokens which were signed with the current access key will also become invalid.

If the organization is not able to rotate the storage account access keys (e.g., the same storage account is used by multiple applications which use the same access key), Mandiant recommends using Azure Storage firewall rules to allow access to the storage account only from a limited set of known and trusted IP addresses. Reference the Azure Storage Hardening Recommendations for additional details.

Azure Storage Account access key rotation using the Azure Portal

1. Go to Azure Portal (https://portal.azure.com).
2. Navigate to the desired storage account.
3. In the left menu, select *Access Keys* to view the access keys for the storage account.
   Note: Each storage account has two storage access keys. If you are not sure which access key is compromised, rotate both access keys.
4. Click the Refresh icon beside each access key for regeneration (see Figure 2)
5. Click "Yes" button to confirm to regenerate the access key.
6. Update the access key in the MOVEit Transfer Config (see Figure 1).

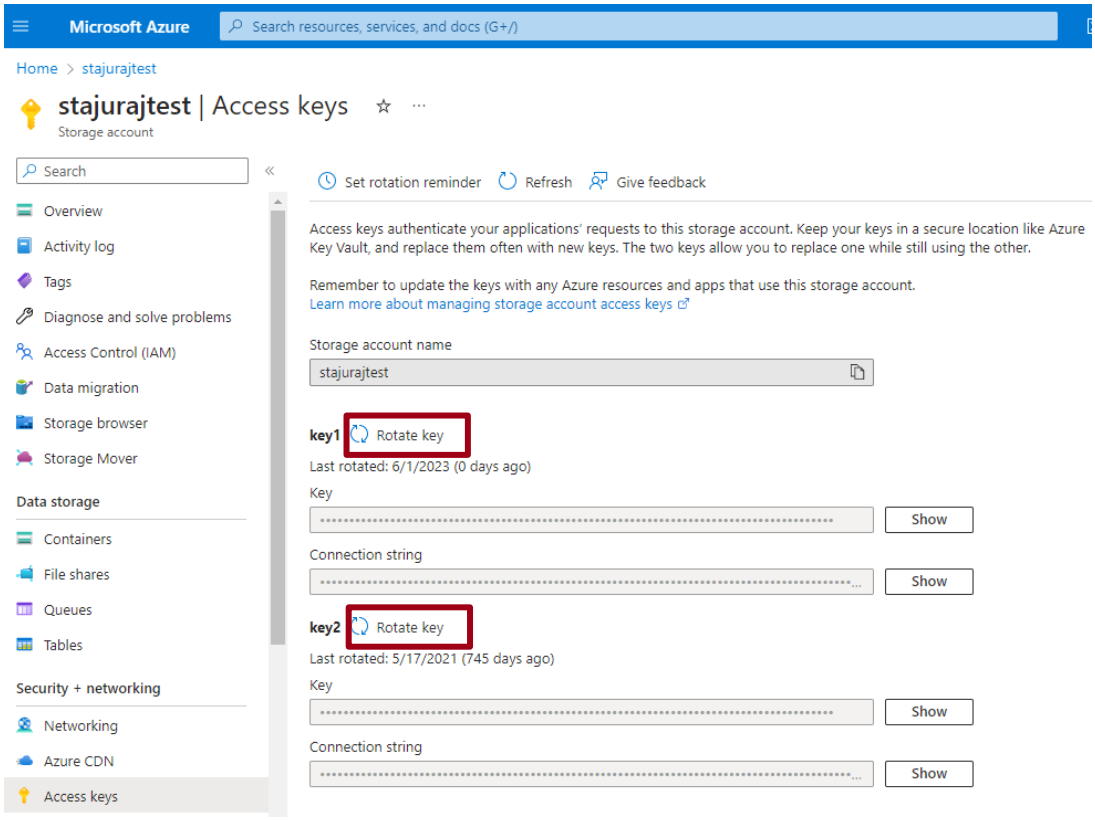

Figure 2 Storage Account Access Keys Regeneration

For additional details for how to manually rotate Azure access keys, reference:

https://learn.microsoft.com/en-us/azure/storage/common/storage-account-keys-manage?tabs=azure-portal#manually-rotate-access-keys

Application and Infrastructure Hardening Recommendations

MOVEit Transfer Application and Architecture Hardening

Goal: Reduce the attack surface and impact to an environment that uses the MOVEit Transfer application.

Account Permissions

Review the listing of permissions that are assigned to local accounts within the MOVEit Transfer application, specifically any accounts that are assigned elevated roles (e.g., GroupAdmin, FileAdmin, Admin, SysAdmin). At a minimum, only a small subset of named accounts should be assigned a privileged role.

Additionally, temporary and guest users should be reviewed, and any dormant accounts associated with these roles should be removed.

For additional information related to permissions, reference:

https://docs.progress.com/bundle/moveit-transfer-web-admin-help-2022/page/permissions.html

Review Password Settings

Within the MOVEit Transfer application, an administrator can set the application's password length and complexity requirements. Mandiant recommends following best practices for password length and complexity even within the application, and to align the password settings to the organization's password policy.

To set the password length and complexity, perform the following steps:

1. Sign-in as Admin
2. In the navigation pane, select Settings
3. Select "Security Policies – Password [Length & Complexity]
4. Enter the Minimum Length requirements associate with your agreed upon organization policy
5. Select Minimum Complexity (choose more than one)

Additionally, MOVEit Transfer can also set specific password configurations for the age and history settings for passwords. These settings can be fine-tuned based on the role (group) an identity has been assigned. Mandiant recommends employing a more stringent password aging and reuse policy for groups that have a higher level of permissions within the application.

For security policies and associated configurations of passwords, reference:

https://docs.progress.com/bundle/moveit-transfer-web-admin-help-2022/page/Security-Policies-Password_2.html

Restrict Network Communications

Depending upon the placement of the server(s) hosting the MOVEit Transfer application, network communications should be restricted (ingress / egress) based upon the concept of deny-by-default. Only the necessary scope of ports and protocols should be permitted for communications to/from the server(s) hosting the MOVEit Transfer

application. The deny-by-default concept can also prevent against potential lateral movement and privilege escalation in the event of a compromise impacting the MOVEit Transfer application.

Figure 3 provides an overview of the recommended connectivity requirements for the application.

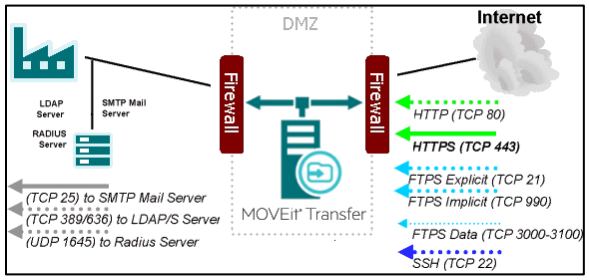

Figure 3: MOVEit Transfer application connectivity requirements via https://docs.progress.com/bundle/moveit-transfer-web-admin-help-2022/page/Firewall-Configuration.html

Remote access policies can also be configured to only allow inbound connections from known and trusted IP addresses.

For additional information related to configuring communications restrictions rulesets for the application, reference:

https://docs.progress.com/bundle/moveit-transfer-web-admin-help-2022/page/firewall-configuration.html

https://docs.progress.com/bundle/moveit-transfer-web-admin-help-2022/page/system-remote-access.htm

https://docs.progress.com/bundle/moveit-transfer-web-admin-help-2022/page/security-policies-remote-access.html

Review Additional Services

The MOVEit Transfer application supports connectivity using additional services such as FTP, FTPs, and SSH. To reduce the attack surface, if these services are not required, they should be administratively disabled. Both the FTP and SSH services can be disabled via the Microsoft Services control panel .

- `MOVEit Transfer FTP service`
- `MOVEit Transfer SSH service`

For additional information related to configuring and managing these additional services, reference:

https://docs.progress.com/bundle/moveit-transfer-web-admin-help-2022/page/FTP-Server.html

https://docs.progress.com/bundle/moveit-transfer-web-admin-help-2022/page/SSH-Server.html

Purge Older Files and Folders

Automated maintenance is a setting (part of nightly scheduled tasks) that can control the cleanup of old files, empty subfolders, aging of new files, and the file quota associated with a folder. This feature can reduce the exposure of potentially sensitive information and files from being accessible in the event of unauthorized access or a vulnerability impacting the MOVEit Transfer application.

For additional information related to configuring and managing Automated Maintenance, reference:

https://docs.progress.com/bundle/moveit-transfer-web-admin-help-2022/page/Automated-Maintenance.html

Note: For any content that is archived within a package, while the data may no longer be accessible to application users, administrators can download and extract archived content. The archive files are present as **unencrypted ZIP files** (`/PACKAGE_ARCHIVE/PROJECT_ARCHIVE-DOWNLOADS`) containing all the packages and associated attachments for the archived period. This can elevate the potential data exposure if package archives are still present, and a threat actor is able to directly access or exfiltrate these files from the environment.

Recommendation: Organizations should develop a process to review and purge un-necessary package archives from the server(s) that host the MOVEit Transfer application

For additional information related to package archives, reference:

https://docs.progress.com/bundle/moveit-transfer-web-admin-help-2023/page/Package-Archives.html

Restrict Inbound Traffic

To further minimize the attack surface of the MOVEit Transfer application, if possible, restrict inbound communications to the MOVEit Transfer application to only **allow-listed** public IP ranges / addresses / domain names. This can be accomplished within the `Remote Access` section of the `System Systems` of the MOVEit Transfer administrative UI. Additionally, custom IP/hostname remote access rules can be configured for particular users.

Note: This recommendation may not be feasible for organizations that have a large scope of distributed customers that need to access the MOVEit application. Additionally, if custom remote access rules are leveraged for users, this can increase the administrative complexity of properly managing the configuration of the MOVEit Transfer application.

For additional information related to these settings, reference:

https://docs.progress.com/bundle/moveit-transfer-web-admin-help-2023/page/Security-Policies-Remote-Access_2.html

Azure Storage Hardening Recommendations

MITRE ATT&CK ID: T1078.004

Goal: Reduce the potential impact of a threat actor directly accessing Azure resources and infrastructure.

Restrict Network Access to Storage Accounts

Mandiant recommends that organizations disable unrestricted network access to Azure storage accounts. Network rules should be configured to only allow approved applications from the organization's Azure virtual networks or from trusted public IP address ranges.

Restricting access to storage accounts will prevent unauthorized access, even in cases where a user's credentials or storage key has inadvertently been exposed. This control will also improve the organization's security posture by allowing approved applications to request data to these storage accounts from a specified set of networks.

As a best practice, avoid using public IPs and use Azure Policy to control the creation of new public IPs. For example, if the business requires public access, the organization could filter the sources to a few specific IP addresses to lock a public IP.

To disable unrestricted network access:

1. Go to Azure Portal.
2. Select Storage account and go to Firewalls and virtual networks.
3. Under "Allow access from", choose Selected networks.

Organizations should also configure the virtual networks and IP address ranges that should be allowed to access the organization's storage accounts.

For additional information related to these configuration options, reference:

https://learn.microsoft.com/en-us/azure/storage/blobs/anonymous-read-access-configure?tabs=portal

Where applicable, Mandiant recommends leveraging private endpoints to access Azure storage from private IPs that do not traverse the public internet. Azure Private Link provides private connectivity from a virtual network to Azure platform as a service (PaaS), customer-owned or Microsoft partner services. Using private endpoints helps to secure connections between endpoints in Azure by eliminating data exposure to the public Internet without the need for an Internet routable IP address.

Disallow Shared Key Authorization Where Not Required

As a best practice, Mandiant recommends disallowing requests to Azure storage accounts using just access keys, and instead authorize the request through Azure AD. Authorizing requests against Azure Storage with Azure AD provides superior security and ease of use over traditional access key authorization. If a threat actor is able to obtain a shared key, the actor would be able to access the storage account directly without using Azure AD to authorize the request.

Mandiant recommends using Azure AD authorization with blob and queue applications, when possible, to minimize potential security vulnerabilities inherent in access key.

For additional information on how to prevent Shared Key authorization for an Azure Storage account, refer to the following link:

https://docs.microsoft.com/en-us/azure/storage/common/shared-key-authorization-prevent?tabs=azure-cli#remediate-authorization-via-shared-key

Monitor Azure Storage Requests

There are a variety of sources to monitor Azure storage accounts. Platform logs provide detailed diagnostic and auditing information for Azure resources and the Azure platform they depend on:

- Resource logs
- Activity logs
- Platform metrics

Platform metrics and the Activity log are collected and stored automatically (for 90 days) and can be routed to other locations by using a diagnostic setting.

Resource Logs are not collected and stored until the organization creates a diagnostic setting to enable and route these logs. To collect resource logs, the organization must create a diagnostic setting. Within the in-scope storage account, select "Diagnostic settings":

1. Select "Add diagnostic setting"
2. Specify one of the following categories of operations for which to collect logs:
    a. StorageRead
    b. StorageWrite
    c. StorageDelete
3. Select the log destination
4. Click Save

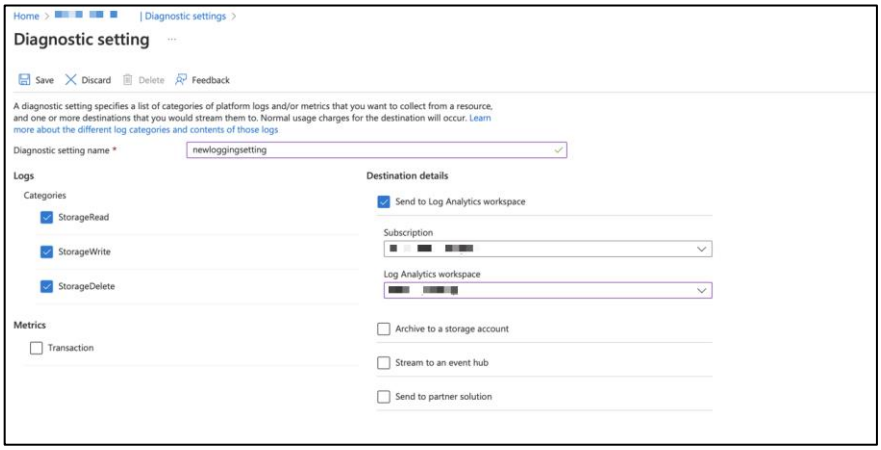

Figure 4: Diagnostic setting

If logs are sent to a Log Analytics workspace, the organization can leverage the following query to identify anonymous requests for a certain time period:

```
StorageBlobLogs
| where TimeGenerated > ago(1d) and AuthenticationType == "Anonymous"
| project TimeGenerated, OperationName, AuthenticationType, Uri
```

Figure 5: List anonymous requests

When the above settings are enabled, the following types of authenticated and anonymous requests are logged:

Authenticated requests

- Successful requests
- Failed requests, including time-out, throttling, network, authorization, and other errors
- Requests that use a shared access signature (SAS) or OAuth, including failed and successful requests
- Requests to analytics data (classic log data in the $logs container and class metric data in the $metric tables)

Anonymous requests

- Successful requests
- Server errors
- Time out errors for both client and server
- Failed GET requests with the error code 304 (Not Modified)

For additional information, reference:

https://learn.microsoft.com/en-us/azure/storage/blobs/blob-storage-monitoring-scenarios

Configure Azure Storage Alerts

Mandiant recommends enabling, monitoring, and responding to security alerts concerning Azure Storage. Two primary sources of alerting are:

Azure Monitor Alerts produce notifications when conditions are met in monitoring data. Alerts can be set on metrics, logs, and the activity log. Sample alerts to configure include:

- High number of anonymous requests to storage container
- GetBlob request from unexpected IP

For information on creating a new alert rule in the Azure portal, reference:

https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-create-new-alert-rule?tabs=metric#create-a-new-alert-rule-in-the-azure-portal

Microsoft Defender for Storage detects anomalous activities indicating unusual and potentially harmful attempts to access storage accounts. Key alerts to configure include:

- Access from a suspicious IP address
- Publicly accessible storage containers successfully discovered
- Access from an unusual location to a storage account
- Potential malware uploaded to a storage account

For a full list of alerts for Microsoft Defender for Storage, reference:

https://learn.microsoft.com/en-us/azure/defender-for-cloud/alerts-reference#alerts-azurestorage

Identify and Reduce the Scope of Privileged Accounts in Active Directory

MITRE ATT&CK ID: T1078

Goal: Reduce the ability for lateral movement using valid credentials from compromised endpoints / services / applications.

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 MOVEit Transfer servers should not be granted permissions to administer Tier 0 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:

```
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 being 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:

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 for 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`

On-Premises Lateral Movement Tactics and Associated Hardening Controls

Goal: Reduce lateral movement capabilities from compromised endpoints / applications / services

Table 2 contains common tactics and the associated hardening controls that can be leveraged to combat against remote access tools and methods from being utilized for lateral movement within an environment.

Tool / Tactic	Mitigating 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)
	
	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
	
	`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)
 	
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.
	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`
	
	Option 2: Windows Firewall Rule enforcement on endpoints
	
	`netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=no`

Tool / Tactic	Mitigating Security Configuration(s)

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
	`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
	`Disable-PSRemoting -Force`
	Option 2: GPO Configuration
	`Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Remote Management (WinRM) > WinRM Service > Allow remote server management through WinRM`
	• `Disabled`
	Option 3: Windows Firewall Rule enforcement on endpoints
	`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.

Tool / Tactic	Mitigating Security Configuration(s)
	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):**
	`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`

Table 2: Common lateral movement tactics and associated hardening controls

IIS Web Server Hardening

Goal: Harden the IIS platform to prevent against additional misconfigurations or compromise.

If the organization has the MOVEit Transfer application on a Windows IIS Server, Mandiant recommends implementing the following hardening measures. Additionally, Progress has published additional IIS hardening measures for consideration (https://community.progress.com/s/article/MOVEit-Transfer-Vulnerability-Scanner-Penetration-Testing-and-Hardening-FAQ-s).

Disable TLS v1.0 and v1.1

Mandiant recommends organizations proactive disable TLS v1.0 and v1.1 as it uses weak cryptography and are not considered secure according to many regulatory standards and frameworks.

The commands referenced in Figure 6 can be used to disable TLS v1.0 using PowerShell.

```
New-Item 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\
TLS 1.0\Server' -Force | Out-Null New-Item
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\ TLS 1.0\Client' -Force
| Out-Null


New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\
TLS 1.0\Server' -name 'Enabled' -value '0' -PropertyType 'DWord' -Force | Out-Null


New-ItemProperty -path
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\ TLS 1.0\Client' -name
'Enabled' -value '0' -PropertyType 'DWord' -Force |
Out-Null


New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\
TLS 1.0\Server' -name 'DisabledByDefault' -value '1' -PropertyType 'DWord' - Force | Out-Null


New-ItemProperty -path
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\ TLS 1.0\Client' -name
'DisabledByDefault' -value '1' -PropertyType 'DWord' - Force | Out-Null
```

Figure 6: Disable TLSv1.0

The commands referenced in Figure 7 Figure 6 can be used to disable TLS v1.1 using PowerShell.

```
New-Item 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\
TLS 1.1\Server' -Force | Out-Null New-Item
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\ TLS 1.1\Client' -Force
| Out-Null
```

```
New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\
TLS 1.1\Server' -name 'Enabled' -value '0' -PropertyType 'DWord' -Force | Out-Null


New-ItemProperty -path
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\ TLS 1.1\Client' -name
'Enabled' -value '0' -PropertyType 'DWord' -Force |
Out-Null


New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\
TLS 1.1\Server' -name 'DisabledByDefault' -value '1' -PropertyType 'DWord' - Force | Out-Null


New-ItemProperty -path
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\ TLS 1.1\Client' -name
'DisabledByDefault' -value '1' -PropertyType 'DWord' - Force | Out-Null
```

Figure 7: Disable TLSv1.1

Limit Critical Information for HTTP Redirect Responses

If the organization has its MOVEit Transfer server behind a Load Balancer or a NAT, there is a possibility of IIS leaking the internal private IP address in the Location HTTP Header redirect response. In order to remediate this issue, ensure that the following HotFix from Microsoft has been applied.

Progress also has published a command that can be leveraged to manually remediate this issue (Figure 8).

```
c:\windows\system32\inetsrv\appcmd.exe set config -section:system.webServer/serverRuntime
/alternateHostName:"[ENTER DOMAIN HERE]" /commit:apphost
```

Figure 8: Command to remediate Information Exposure on HTTP Responses – via https://community.progress.com/s/article/MOVEit-Transfer-Vulnerability-Scanner-Penetration-Testing-and-Hardening-FAQ-s

Require Secure Connections for SessionID Cookies

Progress has noted that a majority of cookies used by Javascript for the MOVEit Transfer application accesses non-critical information, except for the `ASP.NET_SessionId` cookie. This specific cookie should utilize a secure connection with the `HTTPOnly` attribute set to **true**, which is on by default.

To validate that the `ASP.NET_SessionId` cookie is secure, the organization can review via the Developer Console within Browsers or within the application's `web.config` file using the following instructions:

1. Locate and open the application's "`web.config`" file

2. Add the `<httpCookies httpOnlyCookies="true" />` tag within the `<system.web>` section of the file:

```
<configuration> <system.web>
<httpCookies httpOnlyCookies="true" /> </system.web>
</configuration>
```

Figure 9: Ensure 'cookies' are set with the `HttpOnly` attribute

Ensure MIME Type is Declared in Headers

It is recommended that organizations enforce browsers to review the MIME-type declared in an HTTP Header, as opposed to having the browsers review the contents to determine the MIME file type. If it is not declared in the header, this can potentially allow a threat actor to perform a MIME sniffing attack by carefully crafting a file and tricking the browser into interpreting a file as a different MIME type.

This can be configured within IIS by performing the following steps:

1. Open IIS Manager
2. Expand on the site that will be managed
3. Select `HTTP Response Headers`
4. Right-Click the header list and select **Add**
5. Under the **"Name:"** field write "`X-Content-Type-Options`"
6. Under the **"Value:"** field write "`nosniff`"
7. Select **Add** or **Save**

Logging and Hunting Recommendations

Goal: Optimize visibility and enable hunting capabilities to search for evidence of compromise.

Application Logging

The MOVEit Transfer application can forward logged events via SYSLOG or SNMP.
For additional information related to configuring auditing and logging settings, reference:

https://docs.progress.com/bundle/moveit-transfer-web-admin-help-2023/page/System-Auditing.html

Logged activity is also available within the UI, and can be exported in either XML, CSV, or Excel format.

- Users can review their own action history.
- OrgAdmins can review operations for users in their Org.
- SysAdmins can review operations for Orgs.

For additional information related to available logged activity, reference:

https://docs.progress.com/bundle/moveit-transfer-web-admin-help-2022/page/Logs.html

Additionally, IIS web logs and application-specific logs can provide context and information related to application access events.
IIS logs are (by default) present within the following directory on a Windows server:

- `%SystemDrive%\inetpub\logs\LogFiles`

The MOVEit Transfer (DMZ) component will store log files within the location defined within the `Paths` tab of the MOVEit Config application, which is installed on the server running MOVEit DMZ or MOVEit Transfer.

Consider Temporarily increasing the MOVEit DMZ Application logging level to `All Debug`

Potential forensic artifacts, including exploitation time frame, file transfers, and queries, can be found in the `DMZ_ISAPI.log` files. Organizations should consider elevating the logging level to **All Debug**, increasing the log size, and potentially archiving the logs offline in the event that a threat actor attempts to clear local logs.

For additional information related to this setting, reference:

https://docs.ipswitch.com/MOVEit/Transfer2019/Help/Admin/en/index.htm#46482.htm

Consider enabling MySQL General Logging

For systems leveraging MySQL as the database engine, general logging may have been proactively disabled to avoid revealing sensitive customer input. Consider temporarily enabling this logging to identify malicious input that would otherwise not appear in the MOVEit Transfer logs.

For additional information related to this setting, reference:

https://dev.mysql.com/doc/refman/8.0/en/query-log.html

Review IIS Logging Settings

IIS 7.0

IIS Advanced Logging is a module for IIS 7.0 which provides flexibility in logging requests and client data, allowing an organization to configure specific logged parameters for inclusion with IIS log files.

IIS Advanced Logging can be configured for servers, Web sites, and directories in IIS Manager. To enable Advanced Logging using the UI:

1. Open Internet Information Services (IIS) Manager
2. Click the server in the Connections pane
3. Double-click the Logging icon on the Home page
4. Click Select Fields

The fields that will be logged need to be configured using the **Add** or **Edit** Fields button.

Note: This may introduce performance impacts, depending on the extent of the configuration.

IIS 8.5+

IIS version 8.5 (and greater) introduce "Enhanced Logging", which is a default feature that allows for further customization of logging fields for IIS logs.

For enhancing IIS logging configurations, Mandiant recommends adding the `X-FORWARDED-FOR` string from the HTTP request header as a recorded (custom) field for IIS logging (Figure 10). Capturing the X-Forwarded-For header within IIS logs can provide visibility and correlation of the true source IP address of the requesting client, which is especially important when requests traverse multiple network devices (e.g., load balancers and proxy servers).

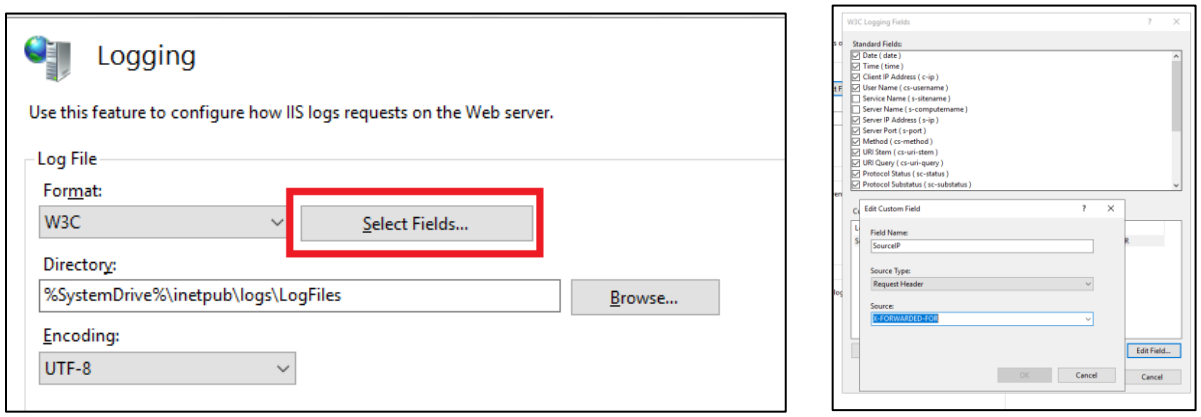

Figure 10: Adding the `X-FORWARDED-FOR` string for HTTP requests within IIS logs

The MOVEit Transfer application also creates several custom HTTP headers that can be configured for logging via the process outlined in Figure 10. Mandiant has observed IOCs and evidence of exfiltration associated with the exploitation of these vulnerabilities in the following custom headers. Organizations should consider adding these headers as a recorded custom field for IIS logging:

- `X-siLock-Comment`
- `X-siLock-SessVar0`
- `X-siLock-SessVar1`
- `X-siLock-SessVar2`
- `X-siLock-SessVar3`
- `X-siLock-SessVar4`
- `X-siLock-SessVar5`
- `X-siLock-SessVar6`

- `X-siLock-Step`
- `X-siLock-Step1`
- `X-siLock-Step2`
- `X-siLock-Step3`
- `X-siLock-Transaction`

Enable Event Tracing for Windows (ETW)

Windows IIS can send logging information to Event Tracing for Windows (ETW). IIS flushes log information to disk, therefore prior to IIS, administrators do not have access to real-time logging information. Text-based log files can also be difficult and time consuming to process. By enabling ETW, administrators have access to use standard query tools for viewing real-time logging information.

To configure ETW logging:

1. Open IIS Manager
2. Select the server or site to enable ETW
3. Select Logging.
4. Ensure Log file format is W3C.
5. Select Both log file and ETW event
6. Save your settings.

Ensure Default IIS Web Logs Location is Moved

IIS will log relatively detailed information on every request. These logs are usually the first item reviewed during a security incident. Threat actors are aware of this valuable information and will often try to remove evidence of their activities. It is therefore recommended that the default location for IIS log files be changed to a restricted, non-system drive.

The following PowerShell script can be used to move the default web log location:

```
Set-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST' -filter
"system.applicationHost/sites/siteDefaults/logFile" -name "directory" -value <new log
location>
```

Figure 11: Move the default IIS web log location to a new directory

To verify if the default web log location has been moved, execute the following command (once entered the attribute “Value” should show the new location of the logs).

```
Get-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST' -filter
"system.applicationHost/sites/siteDefaults/logFile" -name "directory" | select Value
```

Figure 12: Check if the Default IIS web log location was moved

Identify Potential Web Shells (MITRE ATT&CK ID: T1505.003)

Examine WWW root for suspicious files

Search for and analyze any unexpected files in the `c:\MOVEit Transfer\wwwroot\` folder. In particular, examine:

- Dynamic server code files such as aspx, php, and jsf
- Existence of `human2.aspx` (**Note:** `human.aspx` is the original aspx file used by MOVEit).

- Large files
- Files with recent creation timestamps.

Examine `DMZ_WEB.log` for suspicious entries

Look for user activity without any accompanying user login event.

Look for SQL queries that failed due to connection timeouts.

Additionally, look for suspicious SQL queries such as:

- Recent user creations via an "`INSERT INTO users`" command
- Manual session creation via an "`INSERT INTO activesessions`" command, particularly with a localhost IP address
- SQL commands referencing "`Health Check Service`" as a LoginName (not the username)

Examine DMZ_WebApi.log and DMZ_ISAPI.log logs for suspicious entries

Look for exceptions being thrown by incorrect SQLi or improper deserialization.

Look for the following strings:

- `Injection`
- `MyGuestEmailAddr: a@b[.]com`
- `MyPkgSelfProvisionedrecips: ‘);`

Examine WAF and IIS logs for suspicious entries

Examine WAF and IIS logs for suspicious SQL commands such as:

- Recent user creations via an "`INSERT INTO users`" command
- Manual session creation via an "`INSERT INTO activesessions`" command, particularly with a localhost IP address or a timeout value of 9999.
- SQL commands referencing "`Health Check Service`" as a LoginName (not the username)
- Search for Use of the "`X-siLock-Comment`" header with a values that look like GUIDs or other strange entries.

Review MOVEit database tables for suspicious entries

Use the following SQL queries to look for suspicious entries:

```
SELECT * FROM activesessions WHERE Timeout=9999

SELECT Username, realname FROM users WHERE InstID=<NEEDS TO BE CHANGED to the right instID> AND
Permission=30 AND Status='active' and Deleted=0
```

Examine process history for evidence of interactive use of the IUSR account

Compare recent processes created by the IUSR account with a baseline. Certain processes like whoami, netstat, ping, and others are not normally used by built in accounts - and could provide an indicator of potential compromise.

Examine processes spawned by w3wp.exe

The IIS worker processes are hosted by `w3wp.exe`. Some web shells leverage this IIS capability as a persistence or execution mechanism. Suspicious child processes such as `csc.exe`, `cmd.exe`, and `powershell.exe` should be flagged for immediate analysis.

Review database logs for file download events

The MOVEit Transfer application records file interactions within a database table. Investigators can extract file access activity using either the WebUI, or through queries to the underlying database.

Note: As threat actors may clear logs or remove artifacts to hamper an investigation, the methods outlined below may not necessarily provide valid evidence of all activity that occurred during the timeframe of a potential compromise.

WebUI

If available, investigators can leverage the WebUI to review file access activities.

For additional information related to viewing file download activity, reference:

https://docs.progress.com/bundle/moveit-transfer-web-admin-help-2022/page/Recent-Downloads.html

Database Query

Alternatively, investigators can execute the following SQL database query to retrieve file access events.

```
SELECT * FROM log WHERE (LogTime > '2023-05-20 00:00:00')
```

Note: The timeframe for the query should be adjusted to reflect a few days prior to the earliest IOC timestamp related to an investigation. Also, the returned userIDs in the table are not human readable, and will need to be correlated by comparing against the user table in the database.