

MOVEit Transfer Critical Vulnerability (May 2023) (CVE-2023-34362)

Progress has discovered a vulnerability in MOVEit Transfer that could lead to escalated privileges and potential unauthorized access to the environment. If you are a MOVEit Transfer customer, it is extremely important that you take immediate action as noted below in order to help protect your MOVEit Transfer environment.

 Jun 16, 2023 Knowledge

Title

MOVEit Transfer Critical Vulnerability (May 2023) (CVE-2023-34362)

URL Name

MOVEit-Transfer-Critical-Vulnerability-31May2023

Article Number

000234532

Information

Revision History

Date	Description
15-Jun-2023	Added reference to June 15 CVE (CVE-2023-35708)
10-June-2023	Clarified Comments in patch table
09-June-2023	Updated fixed version links, consolidated information can be found on <a href="#">Progress Security Center</a> page Patches updated to include fixes for the Jun 9 CVE
07-June-2023	Updated steps to include removing active sessions, added CISA adv to References, clarified language on APP_WEB_[ <i>random</i> ].dll files
06-June-2023	Updated Cloud versions table to include Test, updated References
05-June-2023	Updated CVE language, updated References to include Microsoft Inte post Added guidance on IIS files to section (2.a iv), updated verbiage on se (2. a i), updated IOCs
04-June-2023	Updated version table to include MOVEit Cloud, converted IOC table .csv, added new IOCs, updated References
03-June-2023	Added Revision History, added upgrade and migration guide, update CVE description, added new Indicators of Compromise, added References
02-June-2023	Added products not impacted Added MOVEit Transfer 2020.1 (12.1) patch information
01-June-2023	
31-May-2023	


SQL Injection ([CVE-2023-35708](#))


In Progress MOVEit Transfer 2022.1.5 (14.1.5), and 2022.1.4 (14.1.4), and 2022.1.3 (14.1.3) MOVEit Transfer web application, an attacker could exploit a vulnerability in MOVEit Transfer's database to access, modify, or delete the contents of the database. NOTE: this is exploited in the wild and can occur via HTTP or HTTPS.


Was this article helpful?





Related Articles

MOVEit Transfer Critical Vulnerability – CVE-2023-35708 (June 15, 2023)  118.41K

WS\_FTP Server Critical Security/Product Alert Bulletin – June 2022  3.09K

WS\_FTP Server is Not Susceptible to the Terrapin SSH Vulnerability  603

MOVEit Transfer Critical Vulnerability – CVE-2023-35036 (June 9, 2023)  38.05K

WS\_FTP Professional is Not Susceptible to the Terrapin SSH Vulnerability  294

Disclaimer

The origins of the information on this site may be internal or external to Progress Software Corporation (“Progress”). Progress Software Corporation makes all reasonable efforts to verify this information. However, the information provided is for your information only. Progress Software Corporation makes no explicit or implied claims to the validity of this information.

Any sample code provided on this site is not supported under any Progress support program or service. The sample code is provided on an "AS IS" basis. Progress makes no warranties, express or implied, and disclaims all implied warranties including, without limitation, the implied warranties of merchantability or of fitness for a particular purpose. The entire risk arising out of the use or performance of the sample code is borne by the user. In no event shall Progress, its employees, or anyone else involved in the creation, production, or delivery of the code be liable for any damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, or other pecuniary loss) or for any use of or inability to use the sample code. Progress has been advised of such potential damages.



We value your privacy

Cookies help make your experience on our website better. We use cookies to personalize content, provide features and analyze our web traffic. Some of these cookies may record user sessions, also help improve and track our promotional and marketing efforts. To see the full list of cookies and learn more please see our [Cookie Policy](#).

Accept and Close

Reject All

Change Settings

mentioned versions are affected, including older unsupported versions.

## Affects

All MOVEit Transfer versions are affected by this vulnerability. See the table below for the security patch for each supported version. Customers on unsupported versions should upgrade to one of the supported fixed versions below.

Based on our review of this situation to date, the following products are not susceptible to this SQL Injection Vulnerability in MOVEit Transfer: MOVEit Automation, MOVEit Client, MOVEit Add-in for Microsoft Outlook, MOVEit Mobile, WS\_FTP Client, WS\_FTP Server, MOVEit EZ, MOVEit Gateway, MOVEit Analytics, MOVEit Freely and any other Progress products. At this time, no action is necessary for the above-mentioned products.

## Recommended Remediation

To help prevent successful exploitation of the mentioned SQLi vulnerability to your MOVEit Transfer environment, we strongly recommend that you immediately apply the following mitigation measures per the steps below.

### 1. Disable all HTTP and HTTPs traffic to your MOVEit Transfer environment

More specifically, modify firewall rules to deny HTTP and HTTPs traffic to MOVEit Transfer on ports 80 and 443 until the patch can be applied.

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

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, please refer to [MOVEit Transfer Help](#).

### 2. Review, Delete and Reset

#### a. Delete Unauthorized Files and User Accounts

- Delete any instances of the human2.aspx (or any files with human2 prefix) and .cmdline script files.
- On the MOVEit Transfer server, look for any new files created in the C:\MOVEitTransfer\wwwroot\ directory.
- On the MOVEit Transfer server, look for new files created in the C:\Windows\TEMP\[random]\ directory with a file extension of [.]cmdline
- On the MOVEit Transfer server, look for new APP\_WEB\_[random].dll files created in the C:\Windows\Microsoft. NET\Framework64\[version]\Temporary ASP .NET Files\root\[random]\[random]\ directory:
  - Stop IIS (iisreset /stop)
  - Delete all APP\_WEB\_[random].dll files located in C:\Windows\Microsoft. NET\Framework64\[version]\Temporary ASP. NET Files\root\[random]\[random]\
  - Start IIS (iisreset /start) **Note:** The next time the web application is accessed they w

#### v. Remove an

[Documenta](#)

#### vi. Remove all

More inform

- Log in
- Naviga
- Select

#### vii. Review logs

files downlo

[Transfer Lo](#)

#### viii. Review IIS l

entries or e



## We value your privacy

Cookies help make your experience on our website better. We use cookies to personalize content, provide features and analyze our web traffic. Some of these cookies may record user sessions, also help improve and track our promotional and marketing efforts. To see the full list of cookies and learn more please see our [Cookie Policy](#).

- ix. If applicable, review Azure logs for unauthorized access to Azure Blob Storage Keys and consider rotating any potentially affected keys.
- b. Reset Service Account Credentials
  - i. Reset service account credentials for affected systems and MOVEit Service Account. See [KB 000115941](#).

3. Apply the Patch

Patches for all supported MOVEit Transfer versions are available below. Supported versions are listed at the following link: <https://community.progress.com/s/products/moveit/product-lifecycle>. Please note, the license file can remain the same to apply the patch.

Affected Version	Fixed Version	Documentation	Comments
MOVEit Transfer 2023.0.0 (15.0)	<a href="#">MOVEit Transfer 2023.0.2 (15.0.2)</a>	<a href="#">MOVEit 2023 Upgrade Documentation</a>	Patches were updated to include fixes for the Jun 9 CVE.
MOVEit Transfer 2022.1.x (14.1)	<a href="#">MOVEit Transfer 2022.1.6 (14.1.6)</a>	<a href="#">MOVEit 2022 Upgrade Documentation</a>	Patches were updated to include fixes for the Jun 9 CVE.
MOVEit Transfer 2022.0.x (14.0)	<a href="#">MOVEit Transfer 2022.0.5 (14.0.5)</a>		
MOVEit Transfer 2021.1.x (13.1)	<a href="#">MOVEit Transfer 2021.1.5 (13.1.5)</a>	<a href="#">MOVEit 2021 Upgrade Documentation</a>	Patches were updated to include fixes for the Jun 9 CVE.
MOVEit Transfer 2021.0.x (13.0)	<a href="#">MOVEit Transfer 2021.0.7 (13.0.7)</a>		
MOVEit Transfer 2020.1.x (12.1)	Special Patch Available	See KB <a href="#">Vulnerability (May 2023) Fix for MOVEit Transfer 2020.1 (12.1)</a>	Patches were updated to include fixes for the Jun 9 CVE.
MOVEit Transfer 2020.0.x (12.0) or older	MUST upgrade to a supported version	<a href="#">See MOVEit Transfer Upgrade and Migration Guide</a>	Patches were updated to include fixes for the Jun 9 CVE.
MOVEit Cloud	Prod: 14.1.6.97 or 14.0.5.45  Test: 15.0.2.39	All MOVEit Cloud systems are fully patched at this time.  <a href="#">Cloud Status Page</a>	Patches were updated to include fixes for the Jun 9 CVE.

4. Verification

- a. To confirm the file transfer is working, follow steps 2A and 2B to reset account credentials.

5. Refer to [MOVEit Transfer](#)

the latest vulnerability fix.

6. Enable all HTTP

7. Continuous Monitoring

- a. Monitor network traffic using the table below.
- 8. Please bookmark this page for latest updates

Additional Security



We value your privacy

Cookies help make your experience on our website better. We use cookies to personalize content, provide features and analyze our web traffic. Some of these cookies may record user sessions, also help improve and track our promotional and marketing efforts. To see the full list of cookies and learn more please see our [Cookie Policy](#).

If you are unable to follow the recommended mitigation steps above, we strongly suggest taking the below security steps to help reduce risk to your MOVEit Transfer environment from unauthorized access. It's important to note, these are not considered mitigation steps to the mentioned vulnerability.

Please see here for [MOVEit Security Best Practices](#).

- **Update network firewall rules** to only allow connections to the MOVEit Transfer infrastructure from known trusted IP addresses.
- **Review and remove any unauthorized user accounts.** See [Progress MOVEit Users Documentation](#) article.
- **Update remote access policies** to only allow inbound connections from known and trusted IP addresses. For more information on restricting remote access, please refer to [SysAdmin Remote Access Rules](#) and [Security Policies Remote Access](#) guide.
- **Allow inbound access only from trusted entities** (e.g., using certificate-based access control).
- **Enable multi-factor authentication.** Multi-factor authentication (MFA) protects MOVEit Transfer accounts from unverified users when a user's account password is lost, stolen, or compromised. To enable MFA, please refer to the [MOVEit Transfer Multi-factor Authentication Documentation](#).

## Indicators of Compromise

See file attachment cve-2023-34362-iocs located at the bottom of this article.

If you do notice any of the indicators noted above, please immediately contact your security and IT teams and open a ticket with Progress Technical Support at:  
<https://community.progress.com/s/supportlink-landing>.

## References

- [MOVEit Security Best Practices Guide](#)
- [Upgrade and/or Migration Guide for MOVEit Automation and MOVEit Transfer](#)
- [CVE-2023-34362 \(NIST\)](#)
- [CVE-2023-34362 \(MITRE\)](#)
- [Mandiant MOVEit Zero-Day Blog](#)
- [Velociraptor - MOVEit CVE-2023-34362 Detection](#)
- [Rapid7 Observed Exploitation of Critical MOVEit Transfer Vulnerability](#)
- [Microsoft Security Intelligence](#)
- [Movin' Out: Identifying Data Exfiltration in MOVEit Transfer Investigations](#)
- [CISA Cyber Security Advisory: #StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability](#)
- [Huntress MOVEit Transfer Critical Vulnerability CVE-2023-34362 Rapid Response](#)

\*Special thank you to Mandiant, Crowdstrike, Rapid7, Microsoft, CISA, and Huntress.

## Additional Information

### Environment

**Last Modified Date**  
6/21/2023 8:29 PM

### Disclaimer

### Defect Number



## We value your privacy

Cookies help make your experience on our website better. We use cookies to personalize content, provide features and analyze our web traffic. Some of these cookies may record user sessions, also help improve and track our promotional and marketing efforts. To see the full list of cookies and learn more please see our [Cookie Policy](#).

 Files (1)

<div><div><div>csv</div></div><div>cve-2023-34362-iocs</div></div>	Jun 21, 2023 • 4KB • csv
<a href="#">View All</a>	