



| Flash |

Reports of Active Exploitation of MOVEit Transfer SQL Zero-Day Vulnerability

F-2023-06-02b

Classification: TLP:CLEAR

Criticality: MEDIUM

Intelligence Requirements: Vulnerability

June 2, 2023

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 8:00 AM (EDT) on June 2, 2023**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Reports of Active Exploitation of MOVEit Transfer SQL Zero-Day Vulnerability

> Key Findings

- A zero-day vulnerability was identified in MOVEit Transfer, a secure managed file transfer software, with reports stating it is being actively exploited in attacks. All MOVEit Transfer versions are affected by this vulnerability.
- The zero-day vulnerability is reported to be a SQL injection vulnerability that can enable threat actors to gain unauthorized access to the environment, escalate privileges, make unauthorized changes to the database, and exfiltrate data from victims. Threat actors have devised a method to leverage this vulnerability to execute arbitrary code.
- ZeroFox Intelligence has not observed significant chatter about this vulnerability on the Deep and Dark Web (DDW). A working Proof-of-Concept (POC) has not been released publicly.
- Customers are advised to implement security patches to supported versions as quickly as possible.

| Analyst Commentary

As early as May 31, 2023, a zero-day vulnerability was disclosed in MOVEit Transfer, a secure managed file transfer software developed by Progress Software Corporation.¹ All MOVEit Transfer versions are affected by this vulnerability, with security patches released for five supported versions.

The vendor stated that the SQL injection vulnerability could enable threat actors to gain unauthorized access to the environment, escalate privileges, make unauthorized changes to the database, and exfiltrate data from victims. The vulnerability has been assigned a Common Vulnerabilities and Exposures (CVE) identification - CVE-2023-34362.

ZeroFox Intelligence has observed multiple open source reports of active exploitation by threat actors, though this has not been independently verified. If these reports are accurate, threat actors will have devised a method to leverage this vulnerability to execute arbitrary code. A list of Indicators of Compromise (IOCs) associated with these reported attacks is included in Appendix A of this report.

ZeroFox Intelligence observed chatter on Reddit and social media environments offering conjecture around the scope and impact of the vulnerability, with individuals claiming to work at impacted organizations identifying multiple randomly named "App_Web_<random>.dll" files, such as "App_Web_feevjhtu.dll", after being breached.²³

ZeroFox Intelligence has observed little chatter on the Deep and Dark Web (DDW) sources or in covert communication channels (e.g., Telegram, IRC) around the vulnerability and has not observed an active Proof-of-Concept shared as of writing. Threat actors have only shared open source news articles on the vulnerability. It is likely that data stolen from victims as a result of this exploit will be sold first in private channels before making its way to DDW community forums. Delays like this are typical to enable

¹ [hXXps://community\[.\]progress\[.\]com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023](https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023)

² [hXXps://www\[.\]reddit\[.\]com/r/msp/comments/13xjsly/tracking_emerging_moveit_transfer_critical/](https://www.reddit.com/r/msp/comments/13xjsly/tracking_emerging_moveit_transfer_critical/)

³ [hXXps://www\[.\]reddit\[.\]com/r/sysadmin/comments/13wxuej/comment/jmhdg55/](https://www.reddit.com/r/sysadmin/comments/13wxuej/comment/jmhdg55/)

the offending threat actors time to maximize profit on stolen data by offering exclusive deals to very trusted associates while avoiding law enforcement and researcher scrutiny.

Security patches have been released for the following MOVEit Transfer versions: 2021.0.x, 2021.1.x, 2022.0.x, 2022.1.x, and 2023.0.0. Users are advised to upgrade to versions 2021.0.6, 2021.1.4, 2022.0.4, 2022.1.5, and 2023.0.1, respectively. If the patches cannot be applied, Progress recommends blocking all HTTP and HTTP traffic to MOVEit Transfer.

| Recommendations

- Delete Unauthorized Files and User Accounts
 - Delete any instances of the human2.aspx 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
 - Remove any unauthorized user accounts. See Progress MOVEit Users Documentation article.
 - Review logs for unexpected downloads of files from unknown IPs or large numbers of files downloaded. For more information on reviewing logs, please refer to the MOVEit Transfer Logs guide.
- Reset service account credentials for affected systems and MOVEit Service Accounts.
- Patch MOVEit Transfer versions: 2021.0.x, 2021.1.x, 2022.0.x, 2022.1.x, and 2023.0.0.
- Users are advised to upgrade to versions 2021.0.6, 2021.1.4, 2022.0.4, 2022.1.5, and 2023.0.1
- Disable all HTTP and HTTPs traffic to your MOVEit Transfer environment.
- Confirm files have been successfully deleted and no unauthorized accounts remain.
- Monitor network, endpoints, and logs for IOCs as listed in the table below
- Utilize the ZeroFox Platform to perform searches on relevant IOCs and further developments.

| Appendix 1: Indicators of Compromise

Type	Indicator
Account	Health Check Service
Filename	human2.aspx
Filename	App_Web_<random>.dll
HTTP Header	X-siLock-Comment
HTTP Header	X-siLock-Step1
HTTP Header	X-siLock-Step2
HTTP Header	X-siLock-Step3
SHA256 Hash	2413b5d0750c23b07999ec33a5b4930be224b661aaf290a0118db803f31acbc5
SHA256 Hash	48367d94ccb4411f15d7ef9c455c92125f3ad812f2363c4d2e949ce1b615429a
SHA256 Hash	6015fed13c5510bbb89b0a5302c8b95a5b811982ff6de9930725c4630ec4011d
SHA256 Hash	702421bcee1785d93271d311f0203da34cc936317e299575b06503945a6ea1e0
SHA256 Hash	9d1723777de67bc7e11678db800d2a32de3bcd6c40a629cd165e3f7bbace8ead
SHA256 Hash	9e89d9f045664996067a05610ea2b0ad4f7f502f73d84321fb07861348fdc24a
SHA256 Hash	b1c299a9fe6076f370178de7b808f36135df16c4e438ef6453a39565ff2ec272
SHA256 Hash	c56bcb513248885673645ff1df44d3661a75cfacdce485535da898aa9ba320d4
SHA256 Hash	d49cf23d83b2743c573ba383bf6f3c28da41ac5f745cde41ef8cd1344528c195
SHA256 Hash	e8012a15b6f6b404a33f293205b602ece486d01337b8b3ec331cd99ccadb562e
IP Address	138.197.152[.]201
IP Address	209.97.137[.]33
IP Address	5.252.191[.]0/24
IP Address	148.113.152[.]144 (reported by community)
IP Address	89.39.105[.]108

| Appendix 2: Detection and Threat Hunting – Sigma Rules

title: MOVEit exploitation

hypothesis: MOVEit affected hosts execute csc.exe via w3wp.exe process to dynamically compile malicious DLL file.

description: >

MOVEit is affected by a critical vulnerability. Exploited hosts show evidence of dynamically compiling a DLL and writing it under

C:\Windows\Microsoft\.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\root\([a-z0-9]{5,12})\([a-z0-9]{5,12})\App_Web_[a-z0-9]{5,12}.dll.

Hunting Opportunity

Events from IIS dynamically compiling binaries via the csc.exe on behalf of the MOVEit application, especially since May 27th should be investigated.

status: experimental

date: 2023/06/01

author: '@kostastsale'

references:

-

<https://www.huntress.com/blog/moveit-transfer-critical-vulnerability-rapid-response>

-

<https://www.trustedsec.com/blog/critical-vulnerability-in-progress-moveit-transfer-technical-analysis-and-recommendations/>

logsource:

category: process_creation

product: windows

detection:

Selection1:

Image|endswith:

- '\csc.exe'

ParentImage|endswith:

- '\w3wp.exe'

Selection2:

ParentCommandLine|contains:

- 'moveitdmz pool'

condition: Selection1 and Selection2

falsepositives:

- "Unknown"

level: medium

tags:

- attack.execution
- attack.T1623

| Appendix 3: Detection and Threat Hunting – Yara Rules

```
rule WEBSHELL_ASPX_DLL_MOVEit_Jun23_1 {
  meta:
    description = "Detects compiled ASPX web shells found being used in MOVEit Transfer
exploitation"
    author = "Florian Roth"
    reference =
"https://www.trustedsec.com/blog/critical-vulnerability-in-progress-moveit-transfer-te
chnical-analysis-and-recommendations/?utm_content=251159938&utm_medium=soci
al&utm_source=twitter&hss_channel=tw-403811306"
    date = "2023-06-01"
    score = 85
    hash1 = "6cbf38f5f27e6a3eaf32e2ac73ed02898cbb5961566bb445e3c511906e2da1fa"
  strings:
    $x1 = "human2_aspx" ascii fullword
    $x2 = "X-siLock-Comment" wide
    $x3 = "x-siLock-Step1" wide
    $a1 = "MOVEit.DMZ.Core.Data" ascii fullword
  condition:
    uint16(0) == 0x5a4d and
    filesize < 40KB and (
      1 of ($x*) and $a1
```

```
    ) or all of them  
}
```

```
rule WEBSHELL_ASPX_MOVEit_Jun23_1 {
```

```
    meta:
```

```
        description = "Detects ASPX web shells as being used in MOVEit Transfer exploitation"
```

```
        author = "Florian Roth"
```

```
        reference =
```

```
"https://www.rapid7.com/blog/post/2023/06/01/rapid7-observed-exploitation-of-critical-  
-moveit-transfer-vulnerability/"
```

```
        date = "2023-06-01"
```

```
        score = 85
```

```
        hash1 = "2413b5d0750c23b07999ec33a5b4930be224b661aaf290a0118db803f31acbc5"
```

```
        hash2 = "48367d94ccb4411f15d7ef9c455c92125f3ad812f2363c4d2e949ce1b615429a"
```

```
        hash3 =
```

```
"e8012a15b6f6b404a33f293205b602ece486d01337b8b3ec331cd99ccadb562e"
```

```
    strings:
```

```
        $s1 = "X-siLock-Comment" ascii fullword
```

```
        $s2 = "]; string x = null;" ascii
```

```
        $s3 = "; if (!String.Equals(pass, " ascii
```

```
    condition:
```

```
        filesize < 150KB and 2 of them
```

```
}
```

```
rule LOG_EXPL_MOVEit_Exploitation_Indicator_Jun23_1 {
```

```
    meta:
```

```
        description = "Detects a possible compromise indicator found in MOVEit Transfer logs"
```

```
        author = "Florian Roth"
```

```
        reference =
```

```
"https://www.huntress.com/blog/moveit-transfer-critical-vulnerability-rapid-response"
```

```
        date = "2023-06-01"
```

```
        score = 70
```

```
    strings:
```

```
        $x1 = "POST /moveitisapi/moveitisapi.dll action=m2 " ascii
```

```
$x2 = " GET /human2.aspx - 443 " ascii  
condition:  
  1 of them  
}
```

| Appendix 4: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.