TLP:AMBER

MOVEit Transfer Sector Update #5 June 16, 2023

Sector Colleagues,

The Office of Cybersecurity and Critical Infrastructure (OCCIP) continues to closely monitor exploitation of the zero-day vulnerability in the managed file transfer (MFT) application MOVEit Transfer, developed by Progress Software Corporation.[1] This vulnerability is tracked as CVE-2023-34362.[2] It does not currently have an associated CVSS score. One new vulnerability was announced June 9. Details on mitigation steps can be found in the mitigation steps section on page 2.

At this time, OCCIP has received a total of ten (10) reports of U.S. financial institutions having been compromised via exploitation of CVE-2023-34362. Additionally, OCCIP continues to gather information indicating the possibility of mass exploitation.

OCCIP has received one confirmed report that CVE-2023-34362 is present in the virtual environment of a major cybersecurity consultancy. Further, there are unconfirmed reports of major financial institutions using MOVEit Transfer in their business operations. Shodan scans reportedly performed by researchers suggest that there are 2,500 web-facing MOVEit Transfer servers globally, which suggests significant utilization of this software by industry.[3] MOVEit Transfer is also leveraged by third parties routinely used by the sector.

OCCIP will continue to collaborate with sector and interagency partners to monitor for exploitation of this vulnerability and will revise its assessment accordingly as more details become available. To aid in your identification and detection efforts, OCCIP would like to highlight the most relevant open-source information about the ongoing exploitation of MOVEit Transfer (below).

OCCIP remains interested in additional information from our stakeholders in the financial services sector on this vulnerability and associated assessments, including reports of compromise as well as potential indicators of compromise your organization may observe. If you would like to provide information, please contact us at OCCIP-Coord@treasury.gov, or through the OCCIP hotline at (202) 622-3000. If you prefer that your information be shared with OCCIP anonymously, please contact the FS-ISAC at sharingops@fsisac.com.

[1] https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023
[2] https://nvd.nist.gov/vuln/detail/CVE-2023-34362; https://www.cve.org/CVERecord?id=CVE-2023-34362
[3] https://www.huntress.com/blog/moveit-transfer-critical-vulnerability-rapid-response

Mitigation Steps:

This information is provided "as-is" for informational purposes only. The Department of the Treasury does not endorse any company, product, or service referenced below, nor does it provide any warranties of any kind regarding the information contained herein.

Official mitigation steps and patched editions of all affected versions of MOVEit Transfer are available at the Progress Software Corporation website for this vulnerability:

Following these mitigation instructions will address previous vulnerabilities.

- MOVEit Transfer Knowledge Base Article (June 9, 2023)

For MOVEit Cloud customers, Progress Software Corporation posted a MOVEit Cloud Knowledge Base Article with more information.

- MOVEit Cloud Knowledge Base Article (June 9, 2023)

Additional References:

CISA notifications:

- The FBI and CISA released an updated Joint Cybersecurity Advisory revising the advisory initially distributed on June 7. This updated document removes old Fortra GoAnywhere Campaign IP addresses and adds new IP addresses. In addition, this product can be found on the FBI's Internet Crime Complaint Center website https://www.ic3.gov/Media/News/2023/230607.pdf.
- (6/7/23) The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) published a joint cybersecurity advisory with technical information on CL0P ransomware gang, also known as TA505, identified through FBI investigations as recently as June 2023.
- (6/2/23) https://www.cisa.gov/news-events/alerts/2023/06/02/cisa-adds-one-known-exploited-vulnerability-catalog
- (6/1/23) https://www.cisa.gov/news-events/alerts/2023/06/01/progress-software-releases-security-advisory-moveit-transfer

Cybersecurity research pages:

- https://www.huntress.com/blog/moveit-transfer-critical-vulnerability-rapid-response
- https://www.rapid7.com/blog/post/2023/06/01/rapid7-observed-exploitation-of-criticalmoveit-transfer-vulnerability/
- https://www.trustedsec.com/blog/critical-vulnerability-in-progress-moveit-transfer-technical-analysis-and-recommendations/

- https://www.tenable.com/blog/cve-2023-34362-moveit-transfer-critical-zero-day-vulnerability exploited-in-the-wild
- https://www.mandiant.com/resources/blog/zero-day-moveit-data-theft

Additional resources:

Since the incident first became widely known, discussion of it has increased across both traditional and social media, including:

- (6/9/23) Newly uncovered evidence suggests that cybercriminals have known about the recently patched MOVEit Transfer zero-day vulnerability since mid-2021.

- (6/8/23) Microsoft is tracking the activity under the moniker Lace Tempest (aka Storm-0950), which has also been implicated in the exploitation of a critical security vulnerability in PaperCut servers.

- (6/7/23) The recently announced MOVEit Transfer vulnerability is a great example (perhaps not, if you are impacted by it) of cyber security attack trends coming together as an extremely effective and damaging exploit.

Indicators of Compromise, available as of June 9, 2023

OCCIP has received indicators of compromise from several sources and will disseminate them to the sector on a rolling basis, as new indicators become available.

SHA-256 Hashes

2413B5D0750C23B07999EC33A5B4930BE224B661AAF290A0118DB803F31ACBC5
48367D94CCB4411F15D7EF9C455C92125F3AD812F2363C4D2E949CE1B615429A
6015FED13C5510BBB89B0A5302C8B95A5B811982FF6DE9930725C4630EC4011D
702421BCEE1785D93271D311F0203DA34CC936317E299575B06503945A6EA1E0
9D1723777DE67BC7E11678DB800D2A32DE3BCD6C40A629CD165E3F7BBACE8EAD
9E89D9F045664996067A05610EA2B0AD4F7F502F73D84321FB07861348FDC24A
B1C299A9FE6076F370178DE7B808F36135DF16C4E438EF6453A39565FF2EC272
C56BCB513248885673645FF1DF44D3661A75CFACDCE485535DA898AA9BA320D4
D49CF23D83B2743C573BA383BF6F3C28DA41AC5F745CDE41EF8CD1344528C195
E8012A15B6F6B404A33F293205B602ECE486D01337B8B3EC331CD99CCADB562E
FE5F8388CCEA7C548D587D1E2843921C038A9F4DDAD3CB03F3AA8A45C29C6A2F
42BBF9EA434C9B90DA12570B645919F8717BC2D589A67EF9824DA14A53B746A2

IP Addresses

5.252.190[.]197
5.252.190[.]0/24
5.252.189-195[.]X
138.197.152[.]201

HTTP Headers

X-siLock-Comment
X-siLock-Step1
X-siLock-Step2
X-siLock-Step3

Filename

human2.aspx

Account

Health Check Service