HC3: Sector Alert

June 2, 2023 TLP:CLEAR Report: 202306021200

Healthcare Sector Potentially at Risk from Critical Vulnerability in MOVEit Transfer Software

Executive Summary

On May 31, 2023, a Progress Software (formerly IPSwitch) published a notification disclosing that a critical vulnerability exists in their MOVEit Transfer software, which could result in unauthorized access and privilege escalation. The vulnerability is a SQL injection flaw that allows for escalated privileges and potential unauthorized access. As of May 31, 2023, the vulnerability does not have a CVE. File transfer solutions are frequently targeted by multiple threat actors, including ransomware groups. Progress Software has yet to report any attempts of extortion due to exposure to the vulnerability, nor is there any attribution to any specific threat actors. However, the exploitation is very similar to the January 2023 mass exploitation of a GoAnywhere MFT zero-day and the December 2020 zero-day exploitation of Accellion FTA servers. Both of these products are managed on file transfer platforms that were heavily exploited by the Clop ransomware gang to steal data and extort organizations.

Impact to HPH Sector

The software is used by multiple organizations in the HPH sector, including hospitals, clinics, and health insurance groups. Sensitive information such as medical records, bank records, social security numbers, and addresses are at risk if this vulnerability is leveraged. The targeted organization could be subject to extortion by finanicially motivated threat groups. HC3 recommends that any HPH organization that currently utilizes MOVEit take immediate action, as noted below in the Mitigations section, while the software company produces a patch.

Report

On May 31, 2023, Progress Software released a security advisory warning customers of a critical vulnerability in MOVEit Transfer software, offering mitigations until patches are installed. The MOVEit Transfer flaw is a SQL injection vulnerability that leads to remote code execution and does not currently have a CVE assigned to it. It is reported that there are 2,500 exposed MOVEit Transfer servers, with the majority located in the U.S., and that the same webshell was found on all exploited devices.

MOVEit Transfer is a leading secure managed file transfer application for collaboration and automated file transfers of sensitive data. It boasts file encryption, security, tamper-evident logging, activity tracking, and centralized access, and helps companies comply with service-level agreements (SLAs), internal governance requirements and regulations like Health Insurance Portability and Accountability Act (HIPAA). Available as a managed service, in the cloud, or on-premise solution, MOVEit consolidates all file transfer activities into one scalable system. Any user can access MOVEit via web, Mac and Windows Desktop clients, or a free mobile app.

According to the software company, hundreds of healthcare organizations, including those in the United States, utilize MOVEit products to deliver scalable, secure, and compliant patient care and business services. These services include healthcare billing, insurance-eligibility inquiries, healthcare claims, detailed audit logs, appointment reminders, patient surveys, and patient retrieval of medical records. The company states that its MOVEit software is the only system to be Federal Information Processing Standard (FIPS) 140-2 certified (the benchmark for validating the effectiveness of cryptographic hardware) by the National Institute of Standards and Technology (NIST). Due to its wide footprint, exploitation of this vulnerability can greatly impact the HPH sector.

HC3: Sector Alert

June 2, 2023 TLP:CLEAR Report: 202306021200

Vulnerabilities

This zero-day vulnerability could allow an attacker to escalate privileges and gain unauthorized access to the healthcare environment, potentially compromising any number of victims.

IOCs	Webshell: human2.asp (location: c:\MOVEit Transfer\wwwroot\ public HTML folder IPs: 138.197.152[.]201 209.97.137[.]33 5.252.191[.]0/24 148.113.152[.]144 89.39.105.108

Yara	Yara Rule for MOVEit Transfer Zero Day (May 31 2023)

Priviledge escalation	Privilege escalation exploits a bug, design flaw or misconfiguration in an operating system or software application to gain elevated access to resources that are normally protected from an application or user. An application with more privileges than intended by the developer or system administrator can perform unauthorized actions.

Unauthorized access	Unauthorized access is when a person gains entry to a computer network, system, application software, data, or other resources without permission. Any access to an information system or network that violates the owner or operator's stated security policy is considered unauthorized access. Unauthorized access is also when legitimate users access a resource that they do not have permission to use.

This vulnerability also follows previous MOVEit vulnerabilites as reported in NIST, including CVE-2023-30394 (May 19, 2023), CVE-2021-37614 (August 17, 2021), CVE-2021-33894 (June 22, 2021), CVE-2021-31827 (May 25, 2021), and CVE-2020-12677 (May 19, 2020).

Patches, Mitigations, and Workarounds

Presently, there are no patches for this latest vulnerability, but there are mitigation measures that can be taken to help prevent unauthorized access to MOVEit Transfer software.

Step 1	**Disable all HTTP and HTTPs traffic to your MOVEit Transfer environment.**
	Modify firewall rules to deny HTTP and HTTPs traffic to MOVEit Transfer on ports 80 and 443. If you require additional support, please immediately contact Progress Technical Support by opening a case via https://community.progress.com/s/supportlink-landing.
	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, please refer to MOVEit Transfer

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

Step 2	**Check for the following potential indicators of unauthorized access over at least the past 30 days:**
	Creation of unexpected files in the c:\MOVEit Transfer\wwwroot\ folder on all your MOVEit Transfer instances (including back-ups)
	Unexpected and/or large file downloads
	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.

Step 3	**Patches for all supported MOVEit Transfer versions are being tested and links will be made available below as they are ready. Supported versions are listed at the following link: https://community.progress.com/s/products/moveit/product-lifecycle.**

The Way Forward

In addition to the aforementioned mitigation strategies and until a patch is released, HC3 recommendations that HPH organizations utilize resources from CISA Stop Ransomware, HHS 405(d), and the H-ISAC to proactively and reactively aid healthcare organizations with cybersecurity awareness and guidance.

The probability of cyber threat actors targeting the healthcare industry remains high. Prioritizing security by maintaining awareness of the threat landscape, assessing their situation, and providing staff with tools and resources necessary to prevent an cyberattack remains the best way forward for healthcare organizations.

References

"IT Solutions: Managed File Transfer Solutions for Healthcare Companies," Progress Community. Accessed June 1, 2023. https://www.ipswitch.com/industries/healthcare

"MOVEit Transfer: Secure Managed File Transfer Software for the Enterprise," Progress Community. Accessed June 1, 2023. https://www.ipswitch.com/moveit-transfer

"MOVEit Transfer Critical Vulnerability (May 2023)," Progress Community. May 31, 2023. https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023?utm_medium

"Progress MOVEit Transfer Critical Vulnerability," NHS 75 Digital. June 1, 2023. https://digital.nhs.uk/cyber-alerts/2023/cc-4326#affected-platforms

"New MOVEit Transfer zero-day mass-exploited in data theft attacks," Bleeping Computer. June 1, 2023. New MOVEit Transfer zero-day mass-exploited in data theft attacks (bleepingcomputer.com)

"Rapid7 Observed Exploitation of Critical MOVEit Transfer Vulnerability," Rapid7. June 1, 2023. Rapid7 Observed Exploitation of Critical MOVEit Transfer Vulnerability | Rapid7 Blog

HC3: Sector Alert

June 2, 2023 TLP:CLEAR Report: 202306021200

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback