HC3: Sector Alert

June 16, 2023 TLP:CLEAR Report: 202306161700

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. An attacker could submit a crafted payload to a MOVEit Transfer application endpoint which could result in modification and disclosure of MOVEit database content. As of June 15, 2023, the vulnerability has been serialized with two separate CVEs: CVE-2023-35708 and CVE 2023-35036. The updates can be found on the Progress Security Center webpage.

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 finanicial motivated threat groups. HC3 recommends that any HPH organization that currently utilizes MOVEit take immediate action as noted below in the Mitigations section as well as applying all updates outlined on the Progress Security Center webpage.

Report

On June 15, 2023, it was reported that multiple local, state, and federal agencies were the target of cyberthreat actors leveraging the MoveIt transfer vulnerabilties. Oregon and Lousiana transporation departments have warned millions of residents their identities are at risk after a cyberattack Thursday stole names, addresses and social security numbers. Two Department of Energy entities were among the of impacted federal agencies. The education sector was also targeted; Johns Hopkins University in Baltimore and the university's renowned health system said in a statement this week that sensitive personal and financial information, including health billing records may have been stolen in the hack. The University of Georgia school system is currently investigating the scope and severity of the hack.

While the exact number of victims remains unknown, CLOP on Wednesday listed the first batch of organizations it says it hacked by exploiting the MOVEit flaw. The victim list, which was posted to Clop's dark web leak site, includes U.S.-based financial services organizations 1st Source and First National Bankers Bank; Boston-based investment management firm Putnam Investments; the Netherlands-based Landal Greenparks; and the U.K.-based energy giant Shell.

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

HC3: Sector Alert

June 16, 2023 TLP:CLEAR Report: 202306161700

	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)

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

All MOVEit Transfer customers must take action and apply the patch to address the June 15th CVE-2023-35708 vulnerability discovered in MOVEit Transfer. There are two paths to take depending on if you have applied the remediation and patching steps from the MOVEit Transfer Critical Vulnerability (May 2023) article prior to June 15.

Step 1	**Have NOT applied May 2023 patch:**
	Follow all the remediation steps and patching in the following article: MOVEit Transfer Critical Vulnerability (May 2023) . That article contains the latest patches, which includes the fix for the June 9 (CVE-2023-35036) vulnerability as well as the original vulnerability from May 31 (CVE-2023-34362).
	After you have done the above, proceed to the Immediate Mitigation Steps below.

Step 2	**Have applied May 2023 (CVE-2023-34362) patch and followed the remediation steps**
	Proceed to the Immediate Mitigation Steps and apply the June 15 patch (CVE Pending) as outlined below. You will then be up to date for the vulnerabilities announced on May 31 (CVE-2023-34362), June 9 (CVE-2023-35036) and June 15 (CVE Pending).
	Have applied May 2023 (CVE-2023-34362) patch, followed the remediation steps and applied the June 9 (CVE-2023-35036) patch
	Proceed to the Immediate Mitigation Steps and apply the June 15 patch (CVE-2023-35708) as outlined below. You will then be up to date for the vulnerabilities announced on May 31 (CVE-2023-34362), June 9 (CVE-2023-35036) and June 15 (CVE-2023-35708).

Immediate Mitigation Steps to Take

To help prevent unauthorized access to your MOVEit Transfer environment, we strongly recommend that you immediately apply the following mitigation measures until you are able to apply the June 15th patch (CVE-2023-35708).

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.
- 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
- SFTP and FTP/s protocols will continue to work as normal

2. 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

3. Apply the Patch
As patches for supported MOVEit Transfer versions become available, links will be provided 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 when staying on a major release to apply the patch.

4. Enable all HTTP and HTTPs traffic to your MOVEit Transfer environment

5. Please bookmark the Progress Security Page and refer to it to ensure you have all of the latest updates.

Way Forward

In addition to the aforementioned mitigation strategies, 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

"MOVEit Transfer Critical Vulnerability – CVE-2023-35708 (June 15, 2023)," Progress Community. Accessed June 16, 2023. https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-15June2023

"US confirms federal agencies hit by MOVEit breach, as hackers list more victims," TechCrunch+. Accessed June 16, 2023. https://techcrunch.com/2023/06/16/us-confirms-federal-agencies-hit-by-moveit-breach-as-hackers-list-more-victims/

"Microsoft says Clop ransomware gang is behind MOVEit mass-hacks, as first victims come forward," TechCrunch+. Accessed June 16, 2023. https://techcrunch.com/2023/06/05/microsoft-clop-moveit-hacks-victims/

"Exclusive: US government agencies hit in global cyberattack," CNN. Accessed June 16, 2023. US government hit in global cyberattack | CNN Politics

"MOVEit Cyber Attack: Personal Data Of Millions Stolen From Oregon, Louisiana, U.S. Agency," Forbes. Accessed June 16, 2023 https://www.forbes.com/sites/maryroeloffs/2023/06/16/moveit-cyber-attack-personal-data-of-millions-stolen-from-oregon-louisiana-us-agency/?sh=7f91ac5f6b05

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