HC3: Sector Alert

June 27, 2024 TLP:CLEAR Report: 202406271500

Critical MOVEit Vulnerabilities Expose Health Sector to Data Breaches

Executive Summary

A critical vulnerability has been identified in MOVEit, a common file transfer platform utilized in the health sector. This vulnerability exposes healthcare organizations to cyberattacks, especially ransomware and data breaches. Progress, the company that owns and operates the MOVEit platform, has released patches to fix this vulnerability. However, exploit code is also available to the public, and this vulnerability is being actively targeted by cyber threat actors. All healthcare organizations are strongly urged to identify any vulnerable instances of MOVEit that exist in their infrastructure and patch them as a high priority.

Analysis

Progress Software, an American business application company, identified and patched two improper authentication vulnerabilities in their MOVEit-managed file transfer (MFT) platform in early June 2024. These vulnerabilities are identical, other than the versions of the MOVEit platform that they affect. Both of them have been patched. (Please see the *Patches, Mitigations, and Workarounds* section below for specifics.) Shortly after the Progress security bulletins were released, WatchTowr labs released further research on one of them – CVE-2024-5806 – which not only provided further details on the vulnerability, but also explored how it might be exploited. WatchTowr also publicly released proof-of-concept exploit code. The company Censys followed this up with research in late June noting that, at the time of publication, they were able to identify 2,700 vulnerable MOVEit MFT instances accessible from the Internet, most of which were physically located in the United States. These vulenrabilities – especially CVE-2024-5806 – should be taken seriously, as they are inherently egregious, but additionally, the MOVEit platform has been previously targeted by highly-capable threat actors on a large scale.

Vulnerabilities

Progress Software identified and patched two vulnerabilities in their MOVEit-managed file transfer platform in early June 2024. These vulnerabilites are:

- CVE-2024-5805 - Improper Authentication vulnerability in Progress' MOVEit Gateway that can allow for authentication bypass. This vulnerability impacts MOVEit Gateway: 2024.0.0.
- CVE-2024-5806 - Improper Authentication vulnerability in Progress' MOVEit Gateway that can allow for authentication bypass. This vulnerability impacts MOVEit Transfer: from 2023.0.0 before 2023.0.11, from 2023.1.0 before 2023.1.6, from 2024.0.0 before 2024.0.2.

These vulnerabilities are identical, other than the versions of the platform they affect. Both of them have been patched. (Please see the *Patches, Mitigations, and Workarounds* section below for specifics.)

Patches, Mitigations, and Workarounds

The security bulletins, including patches for the two vulnerabilities, are located at each of these links:

- MOVEit Gateway Critical Security Alert Bulletin – June 2024 – (CVE-2024-5805)
- MOVEit Transfer Critical Security Alert Bulletin – June 2024 – (CVE-2024-5806)

These patches should be prioritized for deployment.

References

MOVEit Gateway Critical Security Alert Bulletin – June 2024 – (CVE-2024-5805)

https://community.progress.com/s/article/MOVEit-Gateway-Critical-Security-Alert-Bulletin-June-2024-CVE-2024-5805

MOVEit Transfer Critical Security Alert Bulletin – June 2024 – (CVE-2024-5806)
https://community.progress.com/s/article/MOVEit-Transfer-Product-Security-Alert-Bulletin-June-2024-CVE-2024-5806

Auth. Bypass In (Un)Limited Scenarios - Progress MOVEit Transfer (CVE-2024-5806)
https://labs.watchtowr.com/auth-bypass-in-un-limited-scenarios-progress-moveit-transfer-cve-2024-5806/

watchtowrlabs: watchTowr-vs-progress-moveit_CVE-2024-5806
https://github.com/watchtowrlabs/watchTowr-vs-progress-moveit_CVE-2024-5806

Censys: MOVEit Transfer: Auth bypass and a look at exposure
https://censys.com/moveit-transfer-auth-bypass/

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