CERT-EU

Security Advisory 2023-033

Critical Vulnerability in MOVEit Transfer

Jun 19, 2023 — v1.1

TLP:CLEAR

History:

- *02/06/2023 — v1.0 – Initial publication*
- *19/06/2023 — v1.1 – Updated with information regarding the POC and technical details*

Summary

On May 31, 2023, an SQL injection vulnerability has been found in the MOVEit Transfer web application. This critical vulnerability could lead to escalated privileges and potential unauthorised access to the environment. Associated CVE is CVE-2023-34362 with CVSS score of 9.8 [1] and it is actively exploited in the wild [2, 6].

On June 9, 2023, a second patch was released to address several parts of an exploit chain that were not fully mitigated by the first patch. CVE-2023-35036 (CVSS score 9.1) was assigned to the second vulnerability on June 11 [7].

Researchers have released proof-of-concept (PoC) exploit code for CVE-2023-34362 [3], as well as technical root cause analysis of the flaw [4, 5].

CERT-EU highly recommends taking immediate action if you are using this product.

Technical Details

A successful attack could allow unauthenticated remote access to any folder or file within a MOVEit system. Moreover, depending on the database engine being used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker may be able to infer information about the structure and contents of the database in addition to executing SQL statements that alter or delete database elements [4, 5].

Detection

An attacker can leverage the SQLi to clear the database of almost all IOC's. However there is one entry in the database the attacker cannot clear. When performing the final SQLi to delete all IOCs from the database, a single log entry will remain. This log entry is generated after the SQLi is performed and as such cannot be deleted via SQLi.

This log entry will have an Action of `msg_post` and will contain the IP address of the attacker in the `IPAddress` field and a timestamp in the `LogTime` field. The other fields may contain

values the attacker used when performing the SQLi, such as the `MyGuestEmailAddr` value from the forged package used during SQLi.

A strong IOC may be present in the log file `C:\MOVEitTransfer\Logs\DMZ_WebApi.log`. During deserialisation of the malicious gadget an exception of type `TargetInvocationException` will be thrown and the call stack will show the method:

```
MOVEit.DMZ.Application.Folders.ResumableUploadFilePartHandler.DeserializeFileUploadStream
```

which is the method that contains the deserialisation vulnerability [5].

Affected Products

The affected product are:

- MOVEit Transfer before 2023.0.0, 2022.1.x, 2022.0.x, 2021.1.x, 2021.0.x.

Recommendations

To mitigate this vulnerability, upgrade MOVEit Transfer to 2023.0.1, 2022.1.5, 2022.0.4, 2021.1.4 and 2021.0.6.

According to Progress' mitigations [1], before applying the patches, the HTTP (TCP/80) and HTTPS (TCP/443) traffic should be denied to the MOVEit environment and activated after that. Also, any potential unauthorised files or user accounts should be cleaned from the system.

Note that this will block all access to the system, but SFTP/FTP will still work, which currently appears unaffected.

References

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

[2] https://www.trustedsec.com/blog/critical-vulnerability-in-progress-moveit-transfer-technical-analysis-and-recommendations/

[3] https://www.horizon3.ai/moveit-transfer-cve-2023-34362-deep-dive-and-indicators-of-compromise/

[4] https://github.com/horizon3ai/CVE-2023-34362

[5] https://attackerkb.com/topics/mXmV0YpC3W/cve-2023-34362/rapid7-analysis

[6] https://www.helpnetsecurity.com/2023/06/05/cve-2023-34362-exploited/

[7] https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-CVE-2023-35036-June-9-2023