Overall rating: Critical

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware of a SQL injection vulnerability in Progress MOVEit Transfer web application, versions before 2021.0.6 (13.0.6), 2021.1.4 (13.1.4), 2022.0.4 (14.0.4), 2022.1.5 (14.1.5), and 2023.0.1 (15.0.1).

Technical Details

From the NVD (emphasis added):

> a SQL injection vulnerability has been found in the MOVEit Transfer web application that could allow an unauthenticated attacker to gain access to MOVEit Transfer's database. 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, and ***execute SQL statements that alter or delete database elements***. NOTE: ***this is exploited in the wild*** in May and June 2023; ***exploitation of unpatched systems can occur via HTTP or HTTPS***.

*This vulnerability is rated as a **Critical** Severity Threat.*

Indicators of compromise include:

Network Indicators (if observed between March 2023 to present):

- IP Address: 89.39.105[.]108
- IP Address: 5.252.190[.]197
- IP Address: 5.252.190[.]0/24
- IP Address: 5.252.189-195[.]X
- IP Address: 138.197.152[.]201
- IP Address: 209.97.137[.]33

File system Indicators:

Type	Indicator
Account	Health Check Service
Filename	human2.aspx
HTTP Header	X-siLock-Comment
HTTP Header	X-siLock-Step1
HTTP Header	X-siLock-Step2
HTTP Header	X-siLock-Step3

- SHA256 Hash 2413b5d0750c23b07999ec33a5b4930be224b661aaf290a0118db803f31acbc5
- SHA256 Hash 48367d94ccb4411f15d7ef9c455c92125f3ad812f2363c4d2e949ce1b615429a
- SHA256 Hash 6015fed13c5510bbb89b0a5302c8b95a5b811982ff6de9930725c4630ec4011d
- SHA256 Hash 702421bcee1785d93271d311f0203da34cc936317e299575b06503945a6ea1e0
- SHA256 Hash 9d1723777de67bc7e11678db800d2a32de3bcd6c40a629cd165e3f7bbace8ead
- SHA256 Hash 9e89d9f045664996067a05610ea2b0ad4f7f502f73d84321fb07861348fdc24a
- SHA256 Hash b1c299a9fe6076f370178de7b808f36135df16c4e438ef6453a39565ff2ec272
- SHA256 Hash c56bcb513248885673645ff1df44d3661a75cfacdce485535da898aa9ba320d4
- SHA256 Hash d49cf23d83b2743c573ba383bf6f3c28da41ac5f745cde41ef8cd1344528c195
- SHA256 Hash e8012a15b6f6b404a33f293205b602ece486d01337b8b3ec331cd99ccadb562e
- SHA256 Hash fe5f8388ccea7c548d587d1e2843921c038a9f4ddad3cb03f3aa8a45c29c6a2f

If any of these indicators are identified the organization should perform additional investigation for follow-on activity by the threat actors. In several cases, exfiltration of data and additional activity were identified by industry partners.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) if required.
- *Ensure mitigation is performed as soon as possible. Shutting down the system may be a prudent course of action if mitigation cannot occur immediately, because this vulnerability is currently being exploited.*

Please notify VRM with any questions or concerns you may have.

References

NVD - CVE-2023-34362 (nist.gov)
Progress Customer Community
New MOVEit Transfer zero-day mass-exploited in data theft attacks (bleepingcomputer.com)
MOVEit Transfer vulnerability appears to be exploited widely | CSO Online
Rapid7 Observed Exploitation of Critical MOVEit Transfer Vulnerability | Rapid7 Blog