Hive Pro®

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

MOVEit Vulnerabilities Expose Organizations to Cyberattacks

Date of Publication	Admiralty Code	TA Number
October 6, 2023	A1	TA2023402

Summary

First Seen: May 27, 2023
Affected Platform: Progress MOVEit Transfer
Malware: Clop Ransomware
Impact: Critical SQL Injection vulnerabilities in Progress Software's MOVEit Transfer product, exploited by Clop ransomware gang since May 2023, led to unauthorized access and data breaches, affecting numerous organizations worldwide. Millions of individuals may have had their data compromised, revealing the scale of the attack through the exploitation of MOVEit Transfer's vulnerability.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-34362	Progress MOVEit Transfer SQL Injection Vulnerability	Progress MOVEit Transfer	✓	✓	✓
CVE-2023-35036	Progress MOVEit Transfer SQL Injection Vulnerability	Progress MOVEit Transfer	✗	✗	✓
CVE-2023-35708	Progress MOVEit Transfer SQL Injection Vulnerability	Progress MOVEit Transfer	✗	✗	✓
CVE-2023-36934	Progress MOVEit Transfer SQL Injection Vulnerability	Progress MOVEit Transfer	✗	✗	✓
CVE-2023-36932	Progress MOVEit Transfer SQL Injection Vulnerability	Progress MOVEit Transfer	✗	✗	✓
CVE-2023-36933	Progress MOVEit Transfer Unhandled Exception Vulnerability	Progress MOVEit Transfer	✗	✗	✓

Vulnerability Details

#1

The MOVEit Transfer vulnerabilities, initially disclosed by Progress Software in May 2023, include a critical SQL Injection vulnerability (CVE-2023-34362) and two more SQL Injection vulnerabilities (CVE-2023-35036 and CVE-2023-35708), all considered high-risk. In July 2023, a service pack was released to address three additional vulnerabilities (CVE-2023-36934, CVE-2023-36932, and CVE-2023-36933), one of which is critical, while the other two are rated as high-risk.

#2

The exploitation of these vulnerabilities allowed attackers to upload a web shell onto MOVEit Transfer servers, granting them unauthorized access and the ability to perform various malicious activities such as reading configuration data, enumerating files and folders, downloading files, and creating/deleting user accounts.

#3

The attacks began on May 27, 2023, with the Clop ransomware gang being the initial threat actor exploiting the vulnerabilities. Progress Software issued an advisory and patch on May 31, while Clop confirmed their involvement in the attacks on June 5. The FBI and CISA released a joint advisory on June 7, providing information on the attacks and indicators of compromise.

#4

Since the initial disclosure, numerous organizations reported compromises, with Clop adding new victims to their ransomware blog. Clop officially claimed responsibility on June 6 and urged victims to contact them, threatening to publish data from non-compliant organizations.

#5

The full extent of the breach is not fully known, but it potentially affected millions of individuals. The vulnerability in MOVEit impacted supply chains, leading to data breaches involving customer and employee information.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-34362	Progress MOVEit Transfer 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)	cpe:2.3:a:progress:moveit_cloud:*:*:*:*:*:*:*:*	CWE-89
CVE-2023-35036	Progress MOVEit Transfer before 2021.0.7 (13.0.7), 2021.1.5 (13.1.5), 2022.0.5 (14.0.5), 2022.1.6 (14.1.6), and 2023.0.2 (15.0.2)	cpe:2.3:a:progress:moveit_transfer:*:*:*:*:*:*:*:*	CWE-89
CVE-2023-35708	Progress MOVEit Transfer before 2021.0.8 (13.0.8), 2021.1.6 (13.1.6), 2022.0.6 (14.0.6), 2022.1.7 (14.1.7), and 2023.0.3 (15.0.3)	cpe:2.3:a:progress:moveit_transfer:*:*:*:*:*:*:*:*	CWE-89
CVE-2023-36934	Progress MOVEit Transfer before 2020.1.11 (12.1.11), 2021.0.9 (13.0.9), 2021.1.7 (13.1.7), 2022.0.7 (14.0.7), 2022.1.8 (14.1.8), and 2023.0.4 (15.0.4)	cpe:2.3:a:progress:moveit_transfer:*:*:*:*:*:*:*:*	CWE-89
CVE-2023-36932	Progress MOVEit Transfer before 2020.1.11 (12.1.11), 2021.0.9 (13.0.9), 2021.1.7 (13.1.7), 2022.0.7 (14.0.7), 2022.1.8 (14.1.8), and 2023.0.4 (15.0.4	cpe:2.3:a:progress:moveit_transfer:*:*:*:*:*:*:*:*	CWE-89
CVE-2023-36933	Progress MOVEit Transfer before 2021.0.9 (13.0.9), 2021.1.7 (13.1.7), 2022.0.7 (14.0.7), 2022.1.8 (14.1.8), and 2023.0.4 (15.0.4)	cpe:2.3:a:progress:moveit_transfer:*:*:*:*:*:*:*:*	CWE-755

Recommendations

Apply Security Patches and Updates: Organizations using MOVEit Transfer should immediately apply the provided patches and updates to remediate the vulnerabilities. Regularly update all software and applications to mitigate potential security risks.

Vulnerability Scanning and Assessment: Conduct regular vulnerability scans and assessments of your IT infrastructure, including MOVEit Transfer servers. Identify and address any vulnerabilities promptly to reduce the attack surface.

Implement continuous monitoring: Monitor the network, endpoints, and logs for Indicators of Compromise (IoCs) provided by Progress. This helps in detecting and responding to any potential security incidents.

Regular Backups and Disaster Recovery: Implement regular data backups and test your disaster recovery plan. In the event of a ransomware attack, having up-to-date backups can help you recover your data without paying a ransom.

Potential MITRE ATT&CK TTPs

TA0010 Exfiltration	TA0001 Initial Access	TA0005 Defense Evasion	TA0009 Collection
TA0040 Impact	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0002 Execution
TA0008 Lateral Movement	TA0011 Command and Control	TA0042 Resource Development	T1566 Phishing
T1059.001 PowerShell	T1203 Exploitation for Client Execution	T1190 Exploit Public-Facing Application	T1129 Shared Modules
T1505.003 Web Shell	T1546.011 Application Shimming	T1068 Exploitation for Privilege Escalation	T1055 Process Injection

T1070 Indicator Removal	T1574.002 DLL Side-Loading	T1018 Remote System Discovery	T1021.002 SMB/Windows Admin Shares
T1563.002 RDP Hijacking	T1113 Screen Capture	T1071 Application Layer Protocol	T1105 Ingress Tool Transfer
T1041 Exfiltration Over C2 Channel	T1059 Command and Scripting Interpreter	T1486 Data Encrypted for Impact	T1588 Obtain Capabilities
T1588.006 Vulnerabilities	T1588.005 Exploits	T1059.003 Windows Command Shell	

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	5[.]252[.]191[.]103, 5[.]252[.]190[.]117, 209[.]97[.]137[.]33, 5[.]252[.]190[.]100, 5[.]252[.]190[.]244, 5[.]252[.]191[.]31, 5[.]252[.]189[.]130, 165[.]227[.]147[.]215, 5[.]252[.]191[.]241, 5[.]252[.]190[.]119, 5[.]252[.]189[.]210
File Paths	D:\MOVEitDMZ\wwwroot\human2[.]aspx, E:\MOVEitTransfer\wwwroot\human2[.]aspx, C:\Windows\Temp\erymbsqv\erymbsqv[.]dll
SHA256	2413b5d0750c23b07999ec33a5b4930be224b661aaf290a0118db803f31acbc5, 93137272f3654d56b9ce63bec2e40dd816c82fb6bad9985bed477f17999a47db, 7a8f53c4143bacd2104ccd07a6be68d76cda1a6985b8573b7735858a542178bb, c77438e8657518221613fbce451c664a75f05beea2184a3ae67f30ea71d34f37, ba2cf96fc5884cd69ecfe5d73f872958159a12b02ca610223f089ee0b6c3d25d, 5b566de1aa4b2f79f579cdac6283b33e98fdc8c1cfa6211a787f8156848d67ff,

TYPE	VALUE
SHA256	6e1d3b5fcb4de48e1e06a68686817d13533f9740e315f4378bb5b9ef1fd1c7a9, 348e435196dd795e1ec31169bd111c7ec964e5a6ab525a562b17f10de0ab031d, fe5f8388ccea7c548d587d1e2843921c038a9f4ddad3cb03f3aa8a45c29c6a2f, c82059564d6e7a6f56d3b1597cdfe98dfc4e30a2050024bd744f12a3ef237bb5, d477ec94e522b8d741f46b2c00291da05c72d21c359244ccb1c211c12b635899, f994063b9fea6e4b401ee542f6b6d8d6d3b9e5082b5313adbd02c55dc6b4feb7, 2931994f3bde59c3d9da53e0062e4d993dc6fc655a1bd325e90af6dc494ed1fa, 3ff0719da7991a38f508e72e32412a1ee498241bf84f65e973d6e93dc8fd1f66, bdd4fa8e97e5e6eaaac8d6178f1cf4c324b9c59fc276fd6b368e811b327ccf8b, 6015fed13c5510bbb89b0a5302c8b95a5b811982ff6de9930725c4630ec4011d, c56bcb513248885673645ff1df44d3661a75cfacdce485535da898aa9ba320d4, 3a977446ed70b02864ef8cfa3135d8b134c93ef868a4cc0aa5d3c2a74545725b, de4ad0052c273649e0aca573e30c55576f5c1de7d144d1d27b5d4808b99619cd, 3ab73ea9aebf271e5f3ed701286701d0be688bf7ad4fb276cb4fbe35c8af8409, 0ea05169d111415903a1098110c34cdbbd390c23016cd4e179dd9ef507104495, 9e89d9f045664996067a05610ea2b0ad4f7f502f73d84321fb07861348fdc24a, 929bf317a41b187cf17f6958c5364f9c5352003edca78a75ee33b43894876c62, daaa102d82550f97642887514093c98ccd51735e025995c2cc14718330a856f4, f3543cd16de13214124bd7c91033c3cd3bbcf6587871257e699fd89df96fd86f, f0d85b65b9f6942c75271209138ab24a73da29a06bc6cc4faeddcb825058c09d, 3c0dbda8a5500367c22ca224919bfc87d725d890756222c8066933286f26494c, ea433739fb708f5d25c937925e499c8d2228bf245653ee89a6f3d26a5fd00b7a, 24c7fae1b7c02ebd84cc3c78553fb3a68d0466575abea4c92b2f792b47c41ef3,

TYPE	VALUE
SHA256	702421bcee1785d93271d311f0203da34cc936317e299575b06503945a6ea1e0, 387cee566aedbafa8c114ed1c6b98d8b9b65e9f178cf2f6ae2f5ac441082747a, e8012a15b6f6b404a33f293205b602ece486d01337b8b3ec331cd99ccadb562e, cf23ea0d63b4c4c348865cefd70c35727ea8c82ba86d56635e488d816e60ea45, b9a0baf82feb08e42fa6ca53e9ec379e79fbe8362a7dac6150eb39c2d33d94ad, d49cf23d83b2743c573ba383bf6f3c28da41ac5f745cde41ef8cd1344528c195, a1269294254e958e0e58fc0fe887ebbc4201d5c266557f09c3f37542bd6d53d7, 9d1723777de67bc7e11678db800d2a32de3bcd6c40a629cd165e3f7bbace8ead, 87ebfaf36fc7031bec477c70a86cb746811264f530d8af419767b9755e2b43e3, bd45234763ef62f05d14b78c6497ed90706a271fad3b16a4ee6d99d178beedf3, 4359aead416b1b2df8ad9e53c497806403a2253b7e13c03317fc08ad3b0b95bf, b1c299a9fe6076f370178de7b808f36135df16c4e438ef6453a39565ff2ec272
SHA1	12e0643312de827621ec41a6124ded06197a19bc, 794135ba34e99b3c583168a8a15ba09ed869e07e, e7f3f1b8925411a8e33e0dc6e5767cfcda7136f5, 281fb2985d980b8d96a527a06524d9148aa33b54, c063ff83f2c85620637549b8f5c67df84610ce6b, 3f95cebb7a7bd0491912d461208118784f802ca6, fb666835fa6d16fc6e5da965d6e7913358438673, b30dc8a6cb687dea331370963fa8e76183c73511, f1e4d5175d65ba29f200988223f04063fcc28f9d, f3b625622d64e0ccd383f623c0c56ca3c2d820e9, bc215a749524337298f4c5242092838b6eae7e19, 1fdb3aa2979b6595f15a90a1667ca7a6f2e54ea6, 675a908d28570e89b65d06cb4769923353f538da, d972fb8ffb36d16c91cb745d37545e1fa805a931, c1848dab535ae10b8c9542add8a9d74087b629d6, 5b18496a7061dc356bfcdc9c57e82792797db39f, 7bb0bf60b5cd1b42b4774ece368efdf9e759acff, 08561f638b2a2ec2b0eb9871ee30b044e3085fab, ad22b3dea7afedbc304edec373bce41b7247a73e, 4fa0d7b2c6a5a95cf30bf95557089796e1ad271b,

TYPE	VALUE
SHA1	50b575c0d857782b2f76e7198c4c84b0fa60fa8b, 65e8498c0df53a31408665f239b2fb2adeaf7090, 8e5f1af4d2559f509ed1368fd5028e30fbcd64dd, 23f3b810267af1639e9f059536a610798cae1d65, 62103818559cbe4cb9cb58832d8489aa4a09f129, 02f3492857f88824bae7910f171f72fa6def6837, ad8caaab10ea9b378a668ce40bd2e169d0e0dd6d, c48fa2de1ce986c77258c84d9896f3867f8fcc86,

Patch Details

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

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

https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-15June2023

https://community.progress.com/s/article/MOVEit-Transfer-2020-1-Service-Pack-July-2023

References

https://www.progress.com/security/moveit-transfer-and-moveit-cloud-vulnerability

https://www.cisa.gov/news-events/alerts/2023/06/15/progress-software-releases-security-advisory-moveit-transfer-vulnerability

https://unit42.paloaltonetworks.com/threat-brief-moveit-cve-2023-34362/#post-128425-_ydqdbjg0dngh

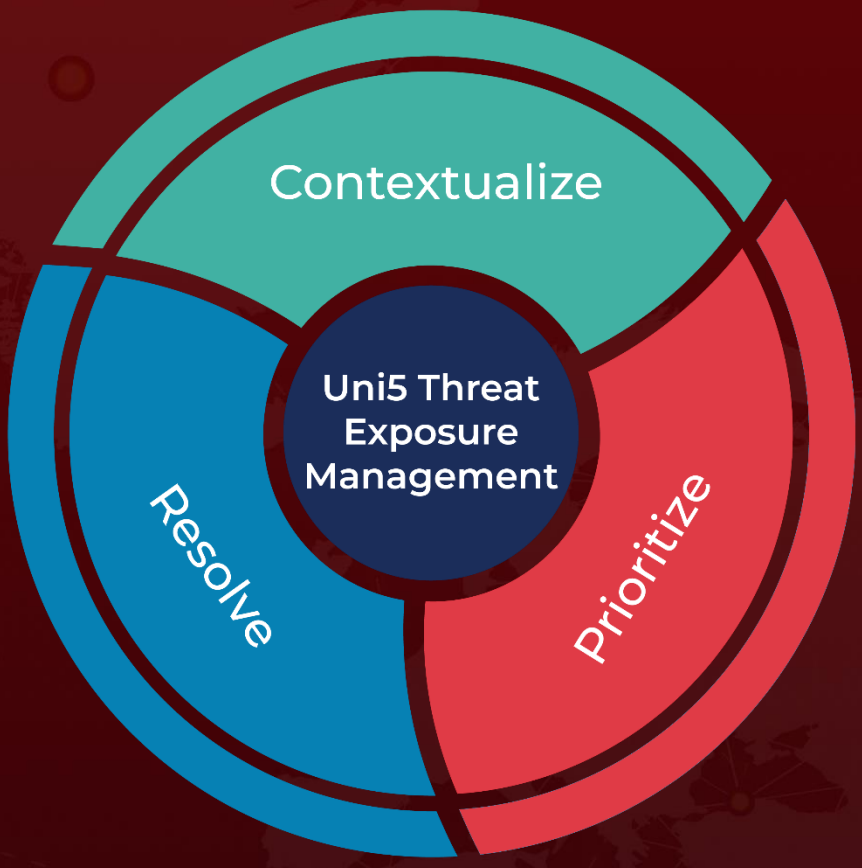
https://www.wired.com/story/moveit-breach-victims/

https://www.hivepro.com/the-exploitation-of-critical-zero-day-vulnerability-found-in-moveit-transfer/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

October 6, 2023 . 6:30 AM

More at www.hivepro.com