CAMENTASYSTEMS

MoveIT Critical Zero-Day Vulnerability

(CVE-2023-34362)

What is MoveIT Vulnerability?

According to open source information, beginning on May 27, 2023, CLOP Ransomware Gang, also known as TA505, began exploiting a previously unknown SQL injection vulnerability (CVE-2023-34362) in Progress Software's managed file transfer (MFT) solution known as MOVEit Transfer. Internet-facing MOVEit Transfer web applications were infected with a web shell named LEMURLOOT, which was then used to steal data from underlying MOVEit Transfer databases. In similar spates of activity, TA505 conducted zero-day-exploit-driven campaigns against Accellion File Transfer Appliance (FTA) devices in 2020 and 2021, and Fortra/Linoma GoAnywhere MFT servers in early 2023.

CVE-2023-34362 MOVEIT TRANSFER VULNERABILITY

MOVEit is typically used to manage an organization's file transfer operations and has a web application that supports MySQL, Microsoft SQL Server, and Azure SQL database engines. In May 2023, the CLOP ransomware group exploited a SQL injection zero-day vulnerability CVE-2023-34362 to install a web shell named LEMURLOOT on MOVEit Transfer web applications [T1190] [1]. Lemurloot was used as a method of persistence, information gathering and data stealing in CVE-2023-34362. The webshell imports multiple libraries including "MOVEit.DMZ.ClassLib," "MOVEit.DMZ.Application.Files," and "MOVEit.DMZ.Application.Users" to interact with MOVEit managed file transfer software. The web shell was initially observed with the name human2.aspx in an effort to masquerade as the legitimate human.aspxfile present as part of MOVEit Transfer software. Upon installation, the web shell creates a random 36 character password to be used for authentication. The web shell interacts with its operators by awaiting HTTP requests containing a header field named X-siLock-Comment, which must have a value assigned equal to the password established upon the installation of the web shell. After authenticating with the web shell, operators pass commands to the web shell that can:

- Retrieve Microsoft Azure system settings, Azure Blob Storage, Azure Blob Storage account, Azure Blob key, and Azure Blob Container using the following query:
  - **"select f.id, f.instid, f.folderid, filesize, f.Name as Name, u.LoginName as uploader, fr.FolderPath , fr.name as fname from folders fr, files f left join users u on f.UploadUsername = u.Username where f.FolderID = fr.ID" (Figure 2).**
- **Enumerate the underlying SQL database.**
- Store a string sent by the operator and then retrieve a file with a name matching the string from the MOVEit Transfer system.

- Create a new administrator privileged account with a randomly generated username and LoginName and RealName values set to "Health Check Service."
- Delete an account with LoginName and RealName values set to 'Health Check Service.'

Why this is important?

Successful exploitation can lead to threat actors with escalated privileges and potential unauthorized access. The Clop ransomware gang claims to have infiltrated hundreds of organizations and provided a June 14 deadline for them to get in touch, possibly to negotiate the price of the stolen data.

How ALISA can help?

ALISA can understand if there is a new header or unusual header with the http or API request. In depth technical details are out of scope of this document, but attackers are using HTTP headers to activate the human2.aspx (which holds the attack details and actually makes the attack).

ALISA AI engine can successfully detect if there is a new header like X-siLock-step1, X-siLock-step2, X-siLock-step3, x-siLock-comment and xX-siLock-comment.

INDICATORS OF COMPROMISE

Type	
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	0ea05169d111415903a1098110c34cdbbd390c23016cd4e179dd9ef507104495
SHA256 Hash	2413b5d0750c23b07999ec33a5b4930be224b661aaf290a0118db803f31acbc5
SHA256 Hash	348e435196dd795e1ec31169bd111c7ec964e5a6ab525a562b17f10de0ab031d
SHA256 Hash	387cee566aedbafa8c114ed1c6b98d8b9b65e9f178cf2f6ae2f5ac441082747a
SHA256 Hash	3a977446ed70b02864ef8cfa3135d8b134c93ef868a4cc0aa5d3c2a74545725b
SHA256 Hash	3ab73ea9aebf271e5f3ed701286701d0be688bf7ad4fb276cb4fbe35c8af8409
SHA256 Hash	4359aead416b1b2df8ad9e53c497806403a2253b7e13c03317fc08ad3b0b95bf
SHA256 Hash	48367d94ccb4411f15d7ef9c455c92125f3ad812f2363c4d2e949ce1b615429a

SHA256 Hash	5b566de1aa4b2f79f579cdac6283b33e98fdc8c1cfa6211a787f8156848d67ff
SHA256 Hash	6015fed13c5510bbb89b0a5302c8b95a5b811982ff6de9930725c4630ec4011d
SHA256 Hash	702421bcee1785d93271d311f0203da34cc936317e299575b06503945a6ea1e0
SHA256 Hash	9d1723777de67bc7e11678db800d2a32de3bcd6c40a629cd165e3f7bbace8ead
SHA256 Hash	9e89d9f045664996067a05610ea2b0ad4f7f502f73d84321fb07861348fdc24a
SHA256 Hash	a1269294254e958e0e58fc0fe887ebbc4201d5c266557f09c3f37542bd6d53d7
SHA256 Hash	b1c299a9fe6076f370178de7b808f36135df16c4e438ef6453a39565ff2ec272

SHA256 Hash	c56bcb513248885673645ff1df44d3661a75cfacdce485535da898aa9ba320d4
SHA256 Hash	c77438e8657518221613fbce451c664a75f05beea2184a3ae67f30ea71d34f37
SHA256 Hash	cf23ea0d63b4c4c348865cefd70c35727ea8c82ba86d56635e488d816e60ea45
SHA256 Hash	d477ec94e522b8d741f46b2c00291da05c72d21c359244ccb1c211c12b635899
SHA256 Hash	d49cf23d83b2743c573ba383bf6f3c28da41ac5f745cde41ef8cd1344528c195
SHA256 Hash	daaa102d82550f97642887514093c98ccd51735e025995c2cc14718330a856f4
SHA256 Hash	e8012a15b6f6b404a33f293205b602ece486d01337b8b3ec331cd99ccadb562e
SHA256 Hash	ea433739fb708f5d25c937925e499c8d2228bf245653ee89a6f3d26a5fd00b7a

SHA256 Hash	f0d85b65b9f6942c75271209138ab24a73da29a06bc6cc4faeddcb825058c09d
SHA256 Hash	fe5f8388ccea7c548d587d1e2843921c038a9f4ddad3cb03f3aa8a45c29c6a2f

As seen from the indicators, those unusual headers can be detected by ALISA in real-time.