2023-06-07

HUNTER

EMERGING THREATS

MOVEIT TRANSFER SQL INJECTION VULNERABILITY (CVE-2023-34362)

CVE-2023-34362 is a critical zero-day vulnerability in the MOVEit Transfer managed file transfer (MFT) software, developed by Progress Software, is being actively exploited. The software, which is used for secure file transfers between business partners and customers, has approximately 1,700 software companies as users, including the US Department of Homeland Security. The vulnerability is a SQL injection flaw that allows attackers to gain unauthorized access, gather information about the database and its contents, and execute SQL statements that can modify, access, or delete database information. Microsoft is attributing attacks exploiting the CVE-2023-34362 MOVEit Transfer 0-day vulnerability to Lace Tempest, known for ransomware operations & running the Clop extortion site

CYBORG SECURITY

THREAT SUMMARY

CVE-2023-34362 is a critical zero-day vulnerability in the MOVEit Transfer managed file transfer (MFT) software, developed by Progress Software, is being actively exploited. The software, which is used for secure file transfers between business partners and customers, has approximately 1,700 software companies as users, including the US Department of Homeland Security. The vulnerability is a SQL injection flaw that allows attackers to gain unauthorized access, gather information about the database and its contents, and execute SQL statements that can modify, access, or delete database information. Microsoft is attributing attacks exploiting the CVE-2023-34362 MOVEit Transfer 0-day vulnerability to Lace Tempest, known for ransomware operations & running the Clop extortion site

The exploitation of this vulnerability has led to the deployment of a web shell, titled "human2.aspx", to be placed in the "wwwroot" directory. This web shell has capabilities that can allow attackers to obtain a list of all folders, files, and users within MOVEit, download any file within MOVEit, and insert an administrative backdoor user into MOVEit, allowing the attacker to maintain persistence. The web shell is also designed to add a new admin user account session with the name "Health Check Service" to maintain further persistence and avoid detection. According to Mandiant, mass exploitation and data exfiltration has occurred over the past few days as a result of this vulnerability. The developer, Progress Software, has released patches for the vulnerability in several versions of the software.

The exploitation of this vulnerability poses a significant risk to organizations using the MOVEit Transfer, as it can lead to unauthorized access, data theft, and potential disruption of services. It is recommended that organizations using MOVEit Transfer take immediate action to mitigate this threat, including installing the provided patches, monitoring for signs of exploitation, and conducting thorough investigations if any indicators of compromise are found.

SYNOPSIS

A critical zero-day vulnerability has been discovered in the MOVEit Transfer managed file transfer (MFT) software, developed by Progress Software. This vulnerability is a SQL injection flaw that enables attackers to gain access to an environment, obtain or modify information about the structure and contents of the database, and execute SQL statements that modify or delete database information. The vulnerability's impact varies depending on the database engine in use, which can be MySQL, Microsoft SQL Server, or Azure SQL. Furthermore, as this vulnerability allows the attacker to execute arbitrary SQL commands, it could lead to full compromise of the MOVEit Transfer database.

Upon successful exploitation of this vulnerability, attackers have been observed deploying a web shell titled "human2.aspx" in the "wwwroot" directory. This web shell is capable of performing several malicious actions, such as obtaining a list of all folders, files, and users within MOVEit, downloading any file within MOVEit environment, and insert an administrative backdoor user into MOVEit to maintain persistence. The web shell also adds a new admin user account session with the name "Health Check Service" to aid in further persistence and detection avoidance. Based on initial analysis of the webshell, it will execute various commands based on the value of the 'X-siLock-Step1', 'X-siLock-Step1', and 'X-siLock-Step3' network request headers.

The exploitation of this vulnerability is widespread and has led to mass downloading of data from organizations, resulting in significant data exfiltration according to Mandiant. The attackers appear to have started exploiting this vulnerability before patches were released by Progress Software, therefore it is advised that impacted organizations thoroughly review their environment for any indicators of compromise to determine if they were targeted. The patches are now available for several versions of the software.

The exploitation of this vulnerability poses a significant threat to organizations using MOVEit Transfer, as it can lead to unauthorized access, data theft, and potential disruption of services. To mitigate this threat, organizations using MOVEit Transfer are advised to install the provided patches, monitor for signs of exploitation, and conduct thorough investigations in case of any indicators of compromise. This includes checking for the presence of the "human2.aspx" web shell, unusual outbound network transfers, and the unauthorized "Health Check Service" user account. In addition to these measures, organizations should also monitor web requests for any of the request or response headers listed in the articles, and check firewall and MOVEit IIS logs for requests from any of the IP addresses specified within the Indicators of Compromise (IOCs) provided in the articles. Cyborg Security's detection engineering and research teams are actively developing Hunt Packages to aid in the detection of this threat, and will update Hunt Packages as new information is released.

HUNT PACKAGES

MOVEIT PRE-COMPILED DLL ARTIFACT FOR WEBSHELL BACKDOOR
https://hunter.cyborgsecurity.io/research/hunt-package/533a2114-1649-43d2-86e3-fef8e600d63d

POSSIBLE MOVEIT MALICIOUS SCRIPT EXECUTION
https://hunter.cyborgsecurity.io/research/hunt-package/5034b751-3866-4c08-b39f-274f49106109

COMPRESSED FILES OR SCRIPTS WRITTEN TO WWWROOT DIRECTORY – POTENTIAL WEBSHELL STAGING ARTIFACTS OR EXFILTRATION
https://hunter.cyborgsecurity.io/research/hunt-package/30E41DFF-ABFE-4429-99E5-6ABC7F2CD764

ENVIRONMENTALLY UNIQUE ASPX FILE WRITTEN TO WWWROOT DIRECTORY – POTENTIAL WEBSHELL INSTALLATION
https://hunter.cyborgsecurity.io/research/hunt-package/a543106e-38fd-4c5b-b266-9343ae82d8cc

RELATED LINKS
Sign up for free HUNTER access
MOVEit Transfer SQL injection Vulnerability (CVE-2023-34362) Emerging Threat Collection

MITRE CONTEXT

- Tactic Names:
  - Initial Access
- Technique Names:
  - Exploit Public-Facing Application
- Threat Names:

REFERENCES

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