Rapid7 Observed Exploitation of Critical MOVEit Transfer Vulnerability

Jun 01, 2023 | 8 min read |

Caitlin Condon

Last updated at Thu, 10 Aug 2023 20:55:31 GMT

***Note:** As of June 2, 2023, CVE-2023-34362 has been assigned to the original MOVEit Transfer zero-day vulnerability. To date, additional MOVEit Transfer CVEs have been disclosed and*

Topics

Metasploit (653)

Vulnerability Management (359)

Research (236)

Detection and Response (205)

Vulnerability Disclosure (148)

Emergent Threat Response (141)

Cloud Security (136)

Security Operations (20)

Popular Tags

Contact Us

Rapid7 recommends updating MOVEit Transfer immediately for all critical CVE releases.

Rapid7 managed services teams are observing exploitation of a critical zero-day vulnerability (CVE-2023-34362) in Progress Software's MOVEit Transfer solution across multiple customer environments. We have observed an uptick in related cases since the vulnerability was disclosed publicly on May 31, 2023; Rapid7 intelligence indicates that the threat actors leveraging CVE-2023-34362 have exploited a wide range of organizations, particularly in North America.

Metasploit

Metasploit Weekly Wrapup

Vulnerability Management

Research

Logentries

Detection and Response

Related Posts

Investigating a SharePoint Compromise: IR Tales from the Field READ MORE

Fortinet FortiManager CVE-2024-47575 Exploited in Zero-Day Attacks READ MORE

Patch Tuesday - October 2024 READ MORE

Contact Us

invoke emergency incident response procedures if any indicators of compromise are found in their environments. Note that while updating to a fixed version will help protect against future exploitation, patching alone is not sufficient to address potential threat actor access to systems that have already been compromised.

Rapid7 has a full in-depth technical analysis of the remote code execution exploit chain for CVE-2023-34362 in AttackerKB

.

Background

Progress Software published an advisory on Wednesday, May 31, 2023 warning of a critical

Command: A Path to Effective Continuous Threat Exposure Management

READ MORE

Contact Us

injection flaw that allows remote attackers to gain unauthorized access to MOVEit Transfer's database. The advisory notes that "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...exploitation of unpatched systems can occur via HTTP or HTTPS."

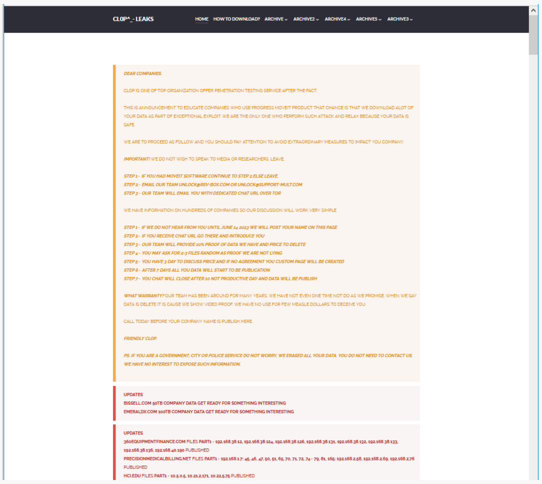
As of June 2, CVE-2023-34362 has been assigned to this issue. The vulnerability was exploited by threat actors at least four days prior to the advisory, and access over "at least the past 30 days."

As a result of large-scale community attention on CVE-2023-34362, Progress Software **released a new patch for CVE-2023-35036, a second SQL injection vulnerability, on Friday, June 9**. One of the files changed appears to be moveitisapi.dll, which our research team confirmed plays a role in the original attack chain. All versions of MOVEit Transfer are affected by this second vulnerability, which is not yet known to be exploited in the wild.

On Thursday, June 15, Progress disclosed a third vulnerability

As of May 31, there were roughly 2,500 instances of MOVEit Transfer exposed to the public internet, the majority of which look to be in the United States. Rapid7 has previously analyzed similar SQLi-to-RCE flaws in network edge systems; these types of vulnerabilities can provide threat actors with initial access to corporate networks. File transfer solutions have also been popular targets for attackers, including ransomware groups, in recent years.

Microsoft attributed the MOVEit Transfer zero-day attacks to Lace Tempest, a threat actor previously linked to Cl0p ransomware, data theft, and extortion attacks. On June them before June 14 to negotiate extortion fees for deleting stolen data. Rapid7 threat intelligence captured the below screenshot of the threat group's demands.



DEAR COMPANIES.

CLOP IS ONE OF TOP ORGANIZATION OFFER PENETRATION TESTING SERVICE AFTER THE FACT.

THIS IS ANNOUNCEMENT TO EDUCATE COMPANIES WHO USE PROGRESS MOVEIT PRODUCT THAT CHANCE IS THAT WE DOWNLOAD ALOT OF YOUR DATA AS PART OF EXCEPTIONAL EXPLOIT. WE ARE THE ONLY ONE WHO PERFORM SUCH ATTACK AND RELAX BECAUSE YOUR DATA IS SAFE.

WE ARE TO PROCEED AS FOLLOW AND YOU SHOULD PAY ATTENTION TO AVOID EXTRAORDINARY MEASURES TO IMPACT YOU COMPANY.

IMPORTANT! WE DO NOT WISH TO SPEAK TO MEDIA OR RESEARCHERS. LEAVE.

STEP 1 - IF YOU HAD MOVEIT SOFTWARE CONTINUE TO STEP 2 ELSE LEAVE.
STEP 2 - EMAIL OUR TEAM UNLOCK@RSV-BOX.COM OR UNLOCK@SUPPORT-MULT.COM
STEP 3 - OUR TEAM WILL EMAIL YOU WITH DEDICATED CHAT URL OVER TOR

WE HAVE INFORMATION ON HUNDREDS OF COMPANIES SO OUR DISCUSSION WILL WORK VERY SIMPLE

STEP 1 - IF WE DO NOT HEAR FROM YOU UNTIL JUNE 14 2023 WE WILL POST YOUR NAME ON THIS PAGE
STEP 2 - IF YOU RECEIVE CHAT URL GO THERE AND INTRODUCE YOU
STEP 3 - OUR TEAM WILL PROVIDE 10% PROOF OF DATA WE HAVE AND PRICE TO DELETE
STEP 4 - YOU MAY ASK FOR 2-3 FILES RANDOM AS PROOF WE ARE NOT LYING
STEP 5 - YOU HAVE 3 DAY TO DISCUSS PRICE AND IF NO AGREEMENT YOU CUSTOM PAGE WILL BE CREATED
STEP 6 - AFTER 7 DAYS ALL YOU DATA WILL START TO BE PUBLICATION
STEP 7 - YOU CHAT WILL CLOSE AFTER 10 NOT PRODUCTIVE DAY AND DATA WILL BE PUBLISH

WHAT WARRANTY? OUR TEAM HAS BEEN AROUND FOR MANY YEARS. WE HAVE NOT EVEN ONE TIME NOT DO AS WE PROMISE. WHEN WE SAY DATA IS DELETE IT IS CAUSE WE SHOW VIDEO PROOF. WE HAVE NO USE FOR FEW MEASLE DOLLARS TO DECEIVE YOU.

CALL TODAY BEFORE YOUR COMPANY NAME IS PUBLISH HERE.

FRIENDLY CLOP.

PS. IF YOU ARE A GOVERNMENT, CITY OR POLICE SERVICE DO NOT WORRY, WE ERASED ALL YOUR DATA. YOU DO NOT NEED TO CONTACT US. WE HAVE NO INTEREST TO EXPOSE SUCH INFORMATION.

UPDATES
BISSELL.COM 50TB COMPANY DATA GET READY FOR SOMETHING INTERESTING
EMERALDX.COM 100TB COMPANY DATA GET READY FOR SOMETHING INTERESTING

UPDATES
360EQUIPMENTFINANCE.COM FILES **PART1 - 192.168.38.12, 192.168.38.124, 192.168.38.126, 192.168.38.131, 192.168.38.132, 192.168.38.133, 192.168.38.136, 192.168.40.190** PUBLISHED
PRECISIONMEDICALBILLING.NET FILES **PART1 - 192.168.1.7: 45, 46, 47, 50, 51, 65, 70, 71, 72, 74 - 79, 81, 165; 192.168.2.58, 192.168.2.69, 192.168.2.76** PUBLISHED
HCI.EDU FILES **PART1 - 10.5.0.5, 10.21.2.171, 10.22.5.75** PUBLISHED

Observed attacker behavior

Rapid7 services teams have so far confirmed indicators of compromise and data exfiltration dating back to at

Contact Us

name in multiple customer environments, which may indicate automated exploitation.

The adversary behavior our teams have observed so far appears to be opportunistic rather than highly targeted; the uniformity of the artifacts we're seeing could plausibly be the work of a single threat actor throwing one exploit indiscriminately at exposed targets. Mandiant has additional analysis supporting this theory here .

Rapid7 analyzed a sample webshell payload associated with successful exploitation. The webshell code would first determine if the inbound request contained a header not populated with a specific password-like value. As of June 1, 2023, all instances of Rapid7-observed MOVEit Transfer exploitation involve the presence of the file `human2.aspx` in the `wwwroot folder` of the MOVEit install directory (`human.aspx` is the native aspx file used by MOVEit for the web interface).

Mitigation guidance

All MOVEit Transfer versions before May 31, 2023 are vulnerable to CVE-2023-34362. Fixed versions of the software are available (see table below), and patches should be applied on an emergency basis. In a patches directly from their knowledge base articles and not from third-party sources.

The below MOVEit Transfer versions were the latest as of June 9, 2023, and included fixes for CVE-2023-34362 and CVE-2023-35036. **NOTE:** New versions are being released to fix CVE-2023-35708 as of June 16. We will update this list as we are able, but please refer to Progress Software's advisory for the latest information.

- MOVEit Transfer 2023.0.2
- MOVEit Transfer 2022.1.6
- MOVEit Transfer 2022.0.5
- MOVEit Transfer 2021.1.5
- MOVEit Transfer 2021.0.7

Contact Us

or older must upgrade to a supported version. Progress software has full up-to-date details and documentation on affected versions, along with installers and DLL drop-ins for fixed versions, in their June 9 advisory . We encourage MOVEit Transfer users to make the May 31 , June 9 , and June 15 advisories their source of ground truth, along with the overview page Progress Software has created.

MOVEit Cloud is also affected and has been patched globally. MOVEit Transfer users who leverage the Microsoft Azure integration should rotate their Azure storage keys.

Contact Us

MOVEit Transfer on ports 80 and 443 until the patch for CVE-2023-34362 can be applied. Users should also delete any unauthorized files or user accounts (e.g., .cmdline scripts, `human2.aspx` instances).

Per the MOVEit advisory , organizations should look for indicators of compromise dating back at least a month. Progress Software also lists IOCs in their advisory.

Identifying data exfiltration

Rapid7 incident response consultants have identified a method to determine what was

Contact Us

EVTX file, which is located at `C:\Windows\System32\winevt\Logs\MOVEit.evtx`. The MOVEit event logs contain a single event ID (Event ID `0`) that provides a plethora of information, including file name, file path, file size, IP address, and username that performed the download.

Progress Software's engineering team told Rapid7 that while event logging is not enabled by default in MOVEit Transfer, it's common for their customers to enable it post-installation. Therefore, many instances of the MOVEit application may have these records available on the host.

Affected organizations and incident responders can use this in meeting regulatory compliance standards where applicable. **NOTE:** It is critical that MOVEit customers capture this log data ***before*** wiping or restoring the application from an earlier backup. Security firm CrowdStrike also has a guide on querying SQL databases directly for exfiltrated data.

Obtaining file download reports from MOVEit Transfer

Rapid7 thanks Progress Software for providing the following information.

The Progress Software team indicated that MOVEit Transfer audit logs are stored in the database and can be either

Contact Us

admin could create a new Custom Report inside of MOVEit with the following values:

Fields: *
Tables: log
Criteria: Action = 'file_download' AND (LogTime LIKE '2023-05%' OR LogTime LIKE '2023-06%')

Saving and running that report would return all File Download actions from the audit log from the months of May and June of this year, with all associated fields. The ‘Fields’ value could then easily be limited to just the relevant data from that point.

Rapid7 customers

InsightVM and Nexpose customers can assess their and remote vulnerability checks. Checks for CVE-2023-35708 are available as of the June 16 content release; InsightVM and Nexpose customers should ensure they are using the latest content version. Authenticated vulnerability checks are supported by both the Scan Engine and the Insight Agent.

The following rules have been added for Rapid7 Insight IDR and Managed Detection Response (MDR) customers:

- Suspicious Web Request - Webshell Related To MOVEit Exploit
- Suspicious Process - MOVEit Transfer Exploitation

Contact Us

Detection .

InsightCloudSec customers can use the ‘Storage Account Older than 90 Days without Access Keys Rotated’ insight to identify Access Keys in need of rotation. Customers can also identify related risk factors, such as resources that are publicly accessible, have encryption disabled, or have threat protection disabled. Custom filtering is available, as well.Finally, InsightCloudSec enables mitigation through bot automation.

Updates

June 3, 2023: Specified exploitation timeline and attacker behavior Rapid7 has

Contact Us

specific vulnerability details.

June 4, 2023: Updated to note that Rapid7 incident responders have identified a method to determine which data and how much was exfiltrated from MOVEit customer environments. Updated to note that MOVEit customers leveraging the Microsoft Azure integration should rotate their storage keys.

June 4, 2023: Updated with guidance on obtaining file download data from MOVEit Transfer — our thanks to the Progress Software team.

June 5, 2023: Updated to note MOVEit Cloud instances are fully patched (Progress Software has asked us to note that cloud instances were patched May 31,

Contact Us

changelog). Also added link to latest vendor update, noted Microsoft attribution. Updated with information on using InsightCloudSec to identify and mitigate risks associated with unrotated Access Keys and unprotected resources.

June 6, 2023: Updated with a summary of the Cl0p gang's extortion demands and the deadline for contact. Added a link to CrowdStrike's guide on identifying exfiltrated data. Made edits for brevity.

June 9, 2023: Updated to note that Progress Software has released new versions of MOVEit Transfer to fix a second vulnerability, whose CVE is still pending. Updated the mitigation

CVEs) and point readers to the advisories and overview page.

June 12, 2023: Updated with Rapid7's full technical analysis of the exploit chain for CVE-2023-34362. InsightVM and Nexpose customers can also now assess their exposure to CVE-2023-35036 with remote and authenticated vulnerability checks.

June 13, 2023: Updated to clarify that Rapid7 has remote and authenticated vulnerability checks available to InsightVM and Nexpose customers for both MOVEit Transfer vulnerabilities (CVE-2023-34362, CVE-2023-35036).

June 15, 2023: Updated to note Progress has disclosed an

June 16, 2023: Updated with CVE-2023-35708 (third MOVEit Transfer vulnerability) information. The full list of latest fixed versions is still pending. Please refer to Progress's advisory for the latest information. InsightVM and Nexpose customers can now assess their exposure to CVE-2023-35708 with both authenticated and remote vulnerability checks available in the June 16 content-only release.

July 7, 2023: Progress Software has disclosed three additional CVEs in MOVEit Transfer as of July 6, 2023. CVE-2023-36934 is a critical SQL injection vulnerability that could allow an unauthenticated attacker to injection vulnerability that could allow authenticated attackers to gain access to the MOVEit Transfer database. CVE-2023-36933 is an exception handling issue that could allow an attacker to crash the application. Fixed versions are available: Mitigation directions and latest versions are in Progress Software's advisory here .

InsightVM and Nexpose customers will be able to assess their exposure to all three CVEs with authenticated vulnerability checks scheduled to be released in the July 7, 2023 content release.

RAPID7

Select

START TRIAL

POST TAGS

Emergent Threat Response

Zero-Day

Vulnerability Management

Detection and Response

SHARING IS CARING

AUTHOR

Caitlin Condon

Director, Vulnerability Intelligence

VIEW CAITLIN'S POSTS

Contact Us

Related Posts

INCIDENT RESPONSE

Investigating a SharePoint Compromise: IR Tales from the Field

READ FULL POST

EMERGENT THREAT RESPONSE

Fortinet FortiManager CVE-2024-47575 Exploited in Zero-Day Attacks

READ FULL POST

VULNERABILITY MANAGEMENT

Patch Tuesday - October 2024

READ FULL POST

VULNERABILITY MANAGEMENT

Modernizing Your VM Program with Rapid7 Exposure Command: A Path to Effective Continuous Threat Exposure Management

READ FULL POST

VIEW ALL POSTS

RAPID7

Select

START TRIAL

Do Not Sell or Share My Personal Information

Cookie Preferences

Contact Us