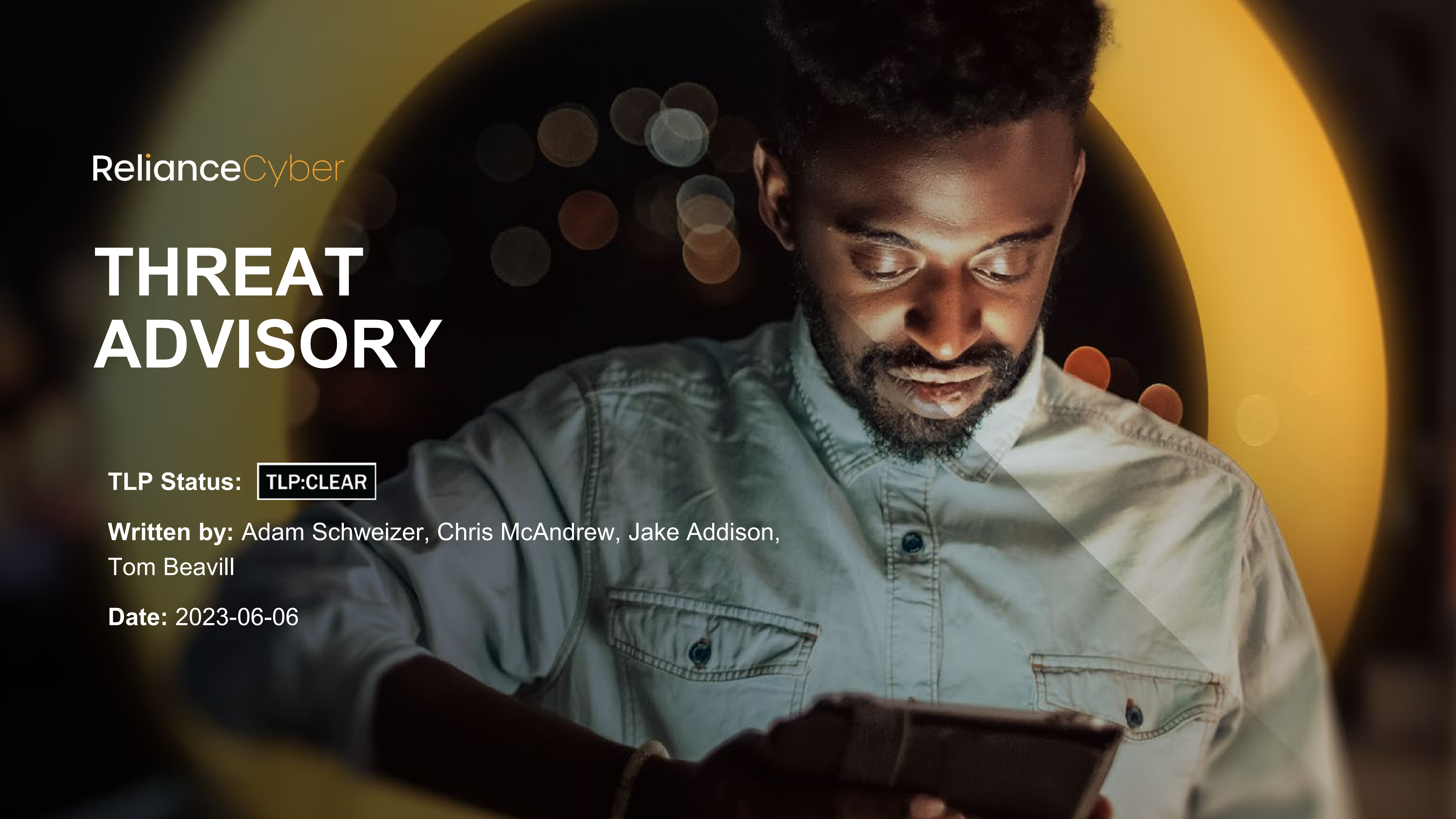

RelianceCyber

THREAT ADVISORY

TLP Status: TLP:CLEAR

Written by: Adam Schweizer, Chris McAndrew, Jake Addison, Tom Beavill

Date: 2023-06-06

RelianceCyber

Widespread Exploitation of MOVEit Transfer Zero-Day Vulnerability

CVE ID	CVE ID Pending
CVSSv3	n/a
Prediction of Exploitation (EPSS)	Actively Exploited
Affected Products	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), 2023.0.1 (15.0.1)
Exploited in the Wild	Yes
Patch Available	Yes

Update – 06/06/2023

A number of important updates have been made by Progress, Crowdstrike, Huntress, Microsoft and Zellis. These are detailed below.

Crowdstrike

- CrowdStrike incident responders have identified evidence of mass file exfiltration from the MOVEit application, as a result of the webshell activity on compromised MOVEit systems
- Data exfiltration activity can be identified by analyzing the MOVEit application database and IIS logs
- See this resource for more details & recommendations - https://www.crowdstrike.com/blog/identifying-data-exfiltration-in-moveit-transfer-investigations/

Widespread Exploitation of MOVEit Transfer Zero-Day Vulnerability

Microsoft

- 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 threat actor has used similar vulnerabilities in the past to steal data & extort victims
- For more details see this resource - https://twitter.com/MsftSecIntel/status/1665537730946670595

Huntress

- Huntress has fully recreated the attack chain exploiting MOVEit Transfer software. To the best of our knowledge, currently no one else has publicly done so.
- We have uncovered that the initial phase of the attack, SQL injection, opens the door for even further compromise -- specifically, arbitrary code execution.
- For more details see this resource – https://www.huntress.com/blog/moveit-transfer-critical-vulnerability-rapid-response

Widespread Exploitation of MOVEit Transfer Zero-Day Vulnerability

Zellis

- Disclosed a data breach related to the vulnerable MOVEit Transfer software
- For more details see this resource - https://www.zellis.com/resources/press-and-media/statement-on-moveit-transfer-data-breach/

The Record (Recorded Future)

- BBC, British Airways and potentially many more affected by data breach at payroll company Zellis
- There were 128 instances of MOVEit Transfer exposed to the internet from the U.K. As a payroll processor, however, Zellis handled data belonging to dozens of other companies, meaning the total number of impacted entities could be significantly higher than those numbers suggest
- For more details see this resource – https://therecord.media/bbc-british-airways-hit-by-zellis-zero-day

Widespread Exploitation of MOVEit Transfer Zero-Day Vulnerability

Progress

- Added Revision History, added upgrade and migration guide, updated CVE description, added new Indicators of Compromise, added References
- Updated version table to include MOVEit Cloud, converted IOC table to .csv, added new IOCs, updated References
- Updated CVE language, updated References to include Microsoft Intel. Post
- Added guidance on IIS files to section (2.a iv), updated verbiage on section (2.a i), updated IOCs
- For more details see this resource – https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023

Widespread Exploitation of MOVEit Transfer Zero-Day Vulnerability

Summary

On June 1, 2023, Rapid7 reported that its managed services teams were observing the active exploitation of a critical, zero-day vulnerability in Progress Software's MOVEit Transfer file transfer solution in multiple of its customers' environments.

Rapid7 disclosed that following the vulnerability's initial disclosure on May 31, 2023, it noticed an increase in attempts to exploit the vulnerability, which is a SQL injection flaw that enables privilege escalation and potentially unauthorized access in target systems.

The vulnerability is new and has not yet been assigned a CVE by MITRE, nor analysed by the National Institute of Standards and Technology (NIST).

While Progress Software did not explicitly indicate in its advisory that the vulnerability had been actively exploited, Rapid7 assessed that language used by the software vendor, specifically its request that Progress Software customers check for indications of unauthorized access in the past 30 days, suggest that the vulnerability may have been exploited prior to its initial disclosure.

According to Shodan scan results, there were approximately 2,500 instances of MOVEit Transfer exposed to the internet at the time of writing.

Widespread Exploitation of MOVEit Transfer Zero-Day Vulnerability

Mandiant CTO Charles Carmakal told BleepingComputer that their data records show that the attacks involving the exploitation of the vulnerability started on May 27, 2023.

Rapid7 noted that it had observed many instances of exploitation of the vulnerability in multiple customer environments in conjunction with the use of webshell X-siLock-Comment, “which may indicate automated exploitation”.

Rapid7 also disclosed that “as of June 1, 2023, all instances of Rapid7-observed MOVEit Transfer exploitation involved the presence of the file human2.aspx (the native aspx file used by MOVEit for the web interface) in the wwwroot folder of the MOVEit install directory”.

Carmakal also stated the following: “Mandiant is currently investigating several intrusions related to the exploitation of the MOVEit managed file transfer zero-day vulnerability.

Mass exploitation and broad data theft has occurred over the past few days. In addition to patching their systems, any organisation using MOVEit Transfer should forensically examine the system to determine if it was already compromised and if data was stolen.

Widespread Exploitation of MOVEit Transfer Zero-Day Vulnerability

Carmakal also suggested that organisations prepare for "*potential extortion and publication of the stolen data*".

Security researcher Kevin Beaumont indicated via Mastodon that the vulnerability very likely also impacts MOVEit Transfer software-as-a-service (SaaS) platform, which would increase the number of potential victims.

MOVEit Transfer Zero Day– Detection

The following IOCs and IOAs are currently noted relating to exploitation of the MOVEit Transfer application.

If you are a Reliance Cyber XDR customer, they are being checked on your network and we will raise an incident if applicable.

IP Addresses / Ranges known to be exploiting or searching for vulnerable servers -

138.197.152[.]201
209.97.137[.]33
5.252.191[.]0/24
148.113.152[.]144 (reported by the community)
89.39.105[.]108

A file which is uploaded to the following directory is a strong indicator of compromise. All files in the wwwroot folder should be checked and confirmed they are expected.

C:\MOVEitTransfer\wwwroot\human2.aspx

A Yara rule has also been released by Florian Roth to check for compiled ASPX web shells found being used in MOVEit Transfer exploitation. https://github.com/Neo23x0/signature-base/blob/master/yara/vuln_moveit_0day_jun23.yar#L2

MOVEit Transfer Zero Day– Recommendations

Reliance Cyber recommends customers take the following steps to help mitigate this threat :

The vendor advisory specifies the following steps to be taken:

Disable all HTTP and HTTPS traffic to your MOVEit Transfer environment

More specifically, modify firewall rules to deny HTTP and HTTPS traffic to MOVEit Transfer on ports 80 and 443 until the patch can be applied.

Review, Delete and Reset

Delete Unauthorized Files and User Accounts
Reset Credentials.

Apply the Patch

Patches for all supported MOVEit Transfer versions are available below. Supported versions are listed at the following link: https://community.progress.com/s/products/moveit/product-lifecycle

MOVEit Transfer Zero Day– Recommendations

Enable all HTTP and HTTPs traffic to your MOVEit Transfer environment

Verification

To confirm the files have been successfully deleted and no unauthorised accounts remain, follow steps 2A again. If you do find indicators of compromise, you should reset the service account credentials again.

Continuous Monitoring

Monitor network, endpoints, and logs for IoCs (Indicators of Compromise) and IoAs (Indicators of Attack) as listed in the table below. For more details, please review page 5.

Reviewing the full advisory is recommended – Advisory Link.

MOVEit Transfer Zero Day–Recommendations

Some community recommendations could also be considered, please see below:

On June 1, 2023, Beaumont suggested users of MOVEit Transfer take 3 actions:

(1) “remove network connectivity/contain”

(2) “check for newly created or altered .asp* files”

(3) and “retain a copy of all IIS logs and network data volume logs”.

Beaumont also suggested the use of Microsoft Safety Scanner to detect malicious webshells that could be used to exploit the vulnerability.

Insikt Group (Recorded Future) Reporting

- https://www.rapid7.com/blog/post/2023/06/01/rapid7-observed-exploitation-of-critical-moveit-transfer-vulnerability/
- https://cyberplace.social/@GossiTheDog/110469042825104814
- https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023
- https://www.reddit.com/r/msp/comments/13xjs1y/tracking_emerging_moveit_transfer_critical/
- https://www.bleepingcomputer.com/news/security/new-moveit-transfer-zero-day-mass-exploited-in-data-theft-attacks/
- https://www.cisa.gov/news-events/alerts/2023/06/01/progress-software-releases-security-advisory-moveit-transfer
- https://therecord.media/moveit-transfer-tool-zero-day-exploited
- https://www.zellis.com/resources/press-and-media/statement-on-moveit-transfer-data-breach/
- https://www.crowdstrike.com/blog/identifying-data-exfiltration-in-moveit-transfer-investigations/
- https://therecord.media/bbc-british-airways-hit-by-zellis-zero-day
- https://www.huntress.com/blog/moveit-transfer-critical-vulnerability-rapid-response
- https://twitter.com/MsftSecIntel/status/1665537730946670595

ReliancCyber

Speak with a consultant

If you would like to speak with one of our consultants directly regarding your security, please:

Get in Touch

RelianceCyber

www.reliancecyber.com