WHITE PAPER

Commvault

Early Warning Signals for Zero-Day Attacks:

A Case Study of the MOVEit and SysAid Vulnerability Exploitation

By Guy Waizel

INTRODUCTION

In May 2023, the CL0P threat group exploited vulnerability CVE-2023-34362 of the MOVEit security file transfer software, which is now commonly known as the 'MOVEit attack' and the 'most impactful zero-day attack of 2023'.[1] Although threat researchers report on early signs of experimentation around this vulnerability as far back as 2021, lines between these early indicators of compromise and the widespread MOVEit attack were drawn only in the aftermath.[2] Numerous organizations and technology providers, including BBC, British Airways, Boots, and many more, are among the victims of this advanced cyber attack.[3] Additionally, the threat group behind the attack previously breached over 130 organizations using another zero-day vulnerability in the GoAnywhere technology.[4] And exploited another zero-day vulnerability in on-prem systems of IT service and helpdesk software SysAid later in November.[5]

IT stakeholders are in an ever-lasting race with cybercriminals to keep their businesses running and data safe from compromise. Commvault helps companies of all industries and sizes adopt a strategy of cyber resilience to protect, defend, and recover data for uninterrupted business continuity.

TIMELINE OF KEY INDICATORS

- **July 2021:** Indicators of compromise are documented in log files. Now, two years later, dots are connected between these early incidents and the CL0P ransomware group assumably experimenting with the exploit for the MOVEit vulnerability before automating it.[6]
- **February 2022:** The same threat group exploits the GoAnywhere-managed file transfer (MFT).[7]
- **April 2022:** Additional indicators of compromise point to experiments with the MOVEit vulnerability exploit.[8]
- **May 27-28th, 2023, Memorial Day holiday:** Numerous organizations are hit by the automated MOVEit attack campaign.[9]
- **May 31st, 2023:** MOVEit software provider Progress discloses the vulnerability, now recorded as CVE-2023-34362.[10]
- **June 7th, 2023:** The CISA and FBI release an advisory #StopRansomware in reaction to the CL0P ransomware group exploiting the MOVEit vulnerability.[11]
- **June 9th, 2023:** A second vulnerability is disclosed by Progress in MOVEit, CVE-2023-35036.[12]
- **June 15th, 2023:** A third vulnerability is disclosed by Progress in MOVEit, CVE-2023-35708, including recommendations for remediation.[13]
- **June 16th, 2023:** CISA confirmed that US government agencies experienced intrusions related to the MOVEit cyber attack.[14]
- **November 8th, 2023:** The CL0P group targets the SysAid server via the vulnerability CVE-2023-47246.[15]
- **January 2024:** Researchers publish numbers that show less than 1% of vulnerabilities contribute to the highest risk and are routinely exploited; their listing includes the MOVEit vulnerability.[16]

PRIMARY INDICATORS OF COMPROMISE FOR INITIAL ACCESS

According to security researchers, the threat actors developed a LEMURLOOT web shell masked with proper filenames such as humans.aspx, to appear as legitimate components of the MOVEit Transfer software. Before interaction with the LEMURLOOT web shell, several POST requests were made to a legitimate file (guestacess.aspx), indicating SQL injection attacks were directed toward that file.[17] [18] The below analysis shows an interaction between two legitimate components of MOVEit Transfer: moveitisapi/moveitisapi.dll and guestaccess.aspx.[19] In Figure 1, we demonstrate how Threatwise can reveal the POST requests made by attackers based on IIS event logs. 'moveitisapi.dll' is used to perform SQL injection when requested with specific headers, and guestaccess.aspx is used to prepare a session and extract CSRF tokens and other field values to perform further actions.[20] Below, we will demonstrate Threatwise detection and alert on similar POST and other web methods requests that were used in interaction with the LEMURLOOT web shell in the very early preparation stage of the attack.

```
2023-05-30 17:05:50 192.168.###.### GET / - 443 - 5.252.190.181 user-agent -
200
2023-05-30 17:06:00 192.168.###.### POST /guestaccess.aspx - 443 -
5.252.191.14 user-agent - 200
2023-05-30 17:06:00 192.168.###.### POST /api/v1/token - 443 - 5.252.191.14
user-agent - 200
2023-05-30 17:06:02 192.168.###.### GET /api/v1/folders - 443 - 5.252.191.14
user-agent - 200 -Example A for ThreatWise detection
2023-05-30 17:06:02 192.168.###.### POST /api/v1/folders/605824912/files
uploadType=resumable 443 - 5.252.191.14 user-agent - 200- Example B for
ThreatWise detection
2023-05-30 17:06:02 ::1 POST /machine2.aspx - 80 - ::1 CWinInetHTTPClient -
200
2023-05-30 17:06:02 192.168.###.### POST /moveitisapi/moveitisapi.dll
action=m2 443 - 5.252.191.14 user-agent - 200-Example C for ThreatWise
detection
2023-05-30 17:06:04 192.168.###.### POST /guestaccess.aspx - 443 -
5.252.190.233 user-agent - 200
2023-05-30 17:06:08 192.168.###.### PUT /api/v1/folders/605824912/files
uploadType=resumable&fileId=963061209 443 - 5.252.190.233 user-agent - 500-
Example D for ThreatWise detection
2023-05-30 17:06:08 ::1 POST /machine2.aspx - 80 - ::1 CWinInetHTTPClient -
200
2023-05-30 17:06:08 192.168.###.### POST /moveitisapi/moveitisapi.dll
action=m2 443 - 5.252.190.233 user-agent - 200
2023-05-30 17:06:11 192.168.###.### POST /guestaccess.aspx - 443 -
5.252.190.116 user-agent - 200
2023-05-30 17:06:21 192.168.###.### GET /human2.aspx - 443 - 5.252.191.88
user-agent - 404
```

Figure 1. IIS Event viewer on an affected host from MOVEit attack[21]

SPOT ATTEMPTS OF VULNERABILITY EXPLOITATION BEFORE A COMPROMISE

With Threatwise, Commvault Cloud provides a lightweight and highly scalable early warning system. Fundamentally different from conventional technologies that analyze interactions looking for known exploits, Threatwise turns the factor of individual network infrastructures and complex architecture of organizational IT into your data protection advantage. By intelligently blanketing on-premises and cloud instances with decoys or threat sensors, malicious activity is spotted early on an inward-out approach along the path to the data. Setting tripwires of fake assets, the sensors mimic tangible IT assets to bait in bad actors away from real resources and data—before data impact.

Threatwise threat sensors record and divert real interactions between threat actors exploiting vulnerabilities and fake assets that send out clear indicators of compromise with comprehensive intelligence data to key IT and security stakeholders across the organization. Event data based on real-time interactions is highly accurate and enhances SIEMs with provisioned attack insights containing minimal false positives, as threat sensors are only visible to malicious users while staying invisible to legitimate employees. The pragmatic early warning alerts record tactics, techniques, and procedures (TTPs) of threat actors' activity and intent, including vulnerability exploitation, stealth techniques, zero-days, and lateral movement. Here are just a few key benefits that help Threatwise users to uncover TTPs as leveraged by the MOVEit attack:

Minimize risk exposure while reducing IT and security teams' cognitive workload. Threatwise strategically layers early warning along the path to your data instances with built-in Threatwise Advisor recommendations. Threatwise Advisor intelligently delegates sensor placement that orchestrates security controls, data protection, and risk governance efforts.

Applied use case: Harden critical workloads such as SQL databases while reducing the cognitive workload for users but continuously scanning backed up data and recommending sensor placement around the backed-up workloads. Protection layers around critical data instances on-prem or on the cloud are validated to expose attackers' intents even before they exploit web and other vulnerabilities of legitimate assets and use SQL injection, such as in the MOVEit and other supply chain zero-day attacks.

Expose threats targeting your business data across the organization by blanketing on-prem and cloud instances in seconds with agentless, preconfigured sensors. Based on one of more than 50 templates from 8 device categories, such as servers, workstations, web decoys, VPN, and industry specifics, threat sensors are deployed in bulk and need no more than an available IP to detect malicious activity on the search for your critical data.

Applied use case: Shielding your organization against malicious intent and activity, the web threat sensor marks web exploitation techniques stored in 3rd party software databases even beyond organizational perimeters. With the sensors' threat intelligence data, you easily spot GET, POST, and PUT requests that are commonly utilized in supply-chain-attacks for vulnerability exploitation, SQL injection to query and manipulate data, and threat actors' customized web shells loaded into 3rd party software (shown in the above examples of LEMURLOOT/MOVEit). Further, any bad actor with privileged access to inside systems that sends web requests to Threatwise threat sensors in DMZ, cloud, or production instances is spotted early – before reaching legitimate systems and data.

Limit the blast radius of a cyber incident and divert early reconnaissance of bad actors seeking your data into flawless duplicates of your real assets, vulnerabilities, and highly unique components. The adaptive sensor provides endless flexibility by fingerprinting existing components and cloning their services, interfaces, and system settings onto a deceptive threat sensor.

Applied use case: By fingerprinting legacy assets with extensive upgrade cycles and known vulnerabilities in the system, the adaptive sensor hides the real component in a crowd of imitations. The sensors create a seamless experience for threat actors scanning the network for vulnerabilities in the search for easy entry points and surface malicious activity at the start.

Stay ahead of the attacker by gathering comprehensive intelligence data about their every move. First, lures or tokens bait in the bad actor from endpoints and strategic network locations. Then, full system and threat sensors based on real systems gather every command, file, and malicious activity across the cyber kill chain. By gaining visibility into the attack, Threatwise provides accurate insights on the latest clean recovery and restore points that ease remediation and recovery.

Applied use case: While occupying the attacker on decoys blended in the system with organizational web interfaces and certificates, valuable intelligence data including an executive summary, attackers' information, malware names, infection sources, and used TTPs according to the MITRE ATT&CK taxonomy is sent to security teams, key IT stakeholders, and security tooling via SIEM integrations enabling to react early.

METHOD USED FOR EARLY DETECTION SIGNALS

In the following figures, we present Threatwise detection alerts for web-based attacks using requests similar to the real affected host IIS event log shown in Figure 1. For this purpose, we utilized cURL, a command-line tool that facilitates data transfer through various protocols, including HTTP. It supports GET, POST, PUT, and other types of requests. cURL is available on most operating systems. In all the tests, Threatwise successfully alerted on malicious activity by an insider threat, capturing the full suite of web requests and all utilized URL paths. Threatwise intelligence data partially includes clear identifications of movitsapi/moveitsapi.dll in the URL. The entire web method and URL request are captured and collected in the management console for further analysis and documentation. If MOVEit is not installed on the sensor, the request does not fully succeed for the attacker; however, the event with the request and the full URL is recorded and presented in Threatwise.

EARLY WARNING SIGNALS OF A ZERO-DAY ATTACK USING THREATWISE

Example A: Related with IIS Event:" GET /api/v1/folders"
(see Figure 1, Example A)

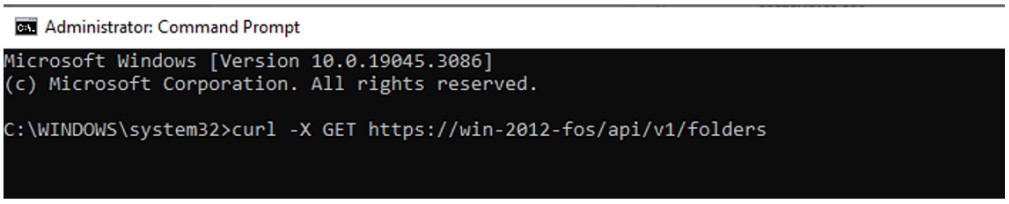

Figure 2: Example A. Sending a GET request to a Threatwise Web decoy URL using curl command resulting in a similar IIS event as in Figure 1, example A

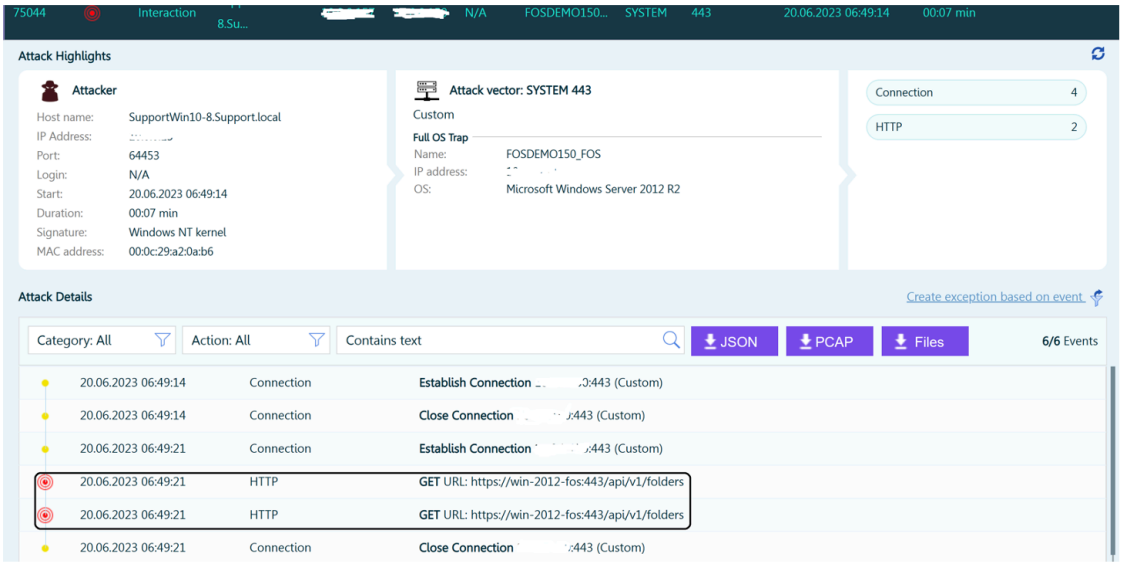

Figure3: Threatwise detection of GET requests sent to the decoy

Example B: Related with IIS Event "POST /api/v1/folders/605824912/files upload Type=resumable"
(see Figure1. Example B)

Figure 4: Example B. Sending a POST request to a decoy URL and uploading a file resulting in a similar IIS event as in Figure 1. Example B

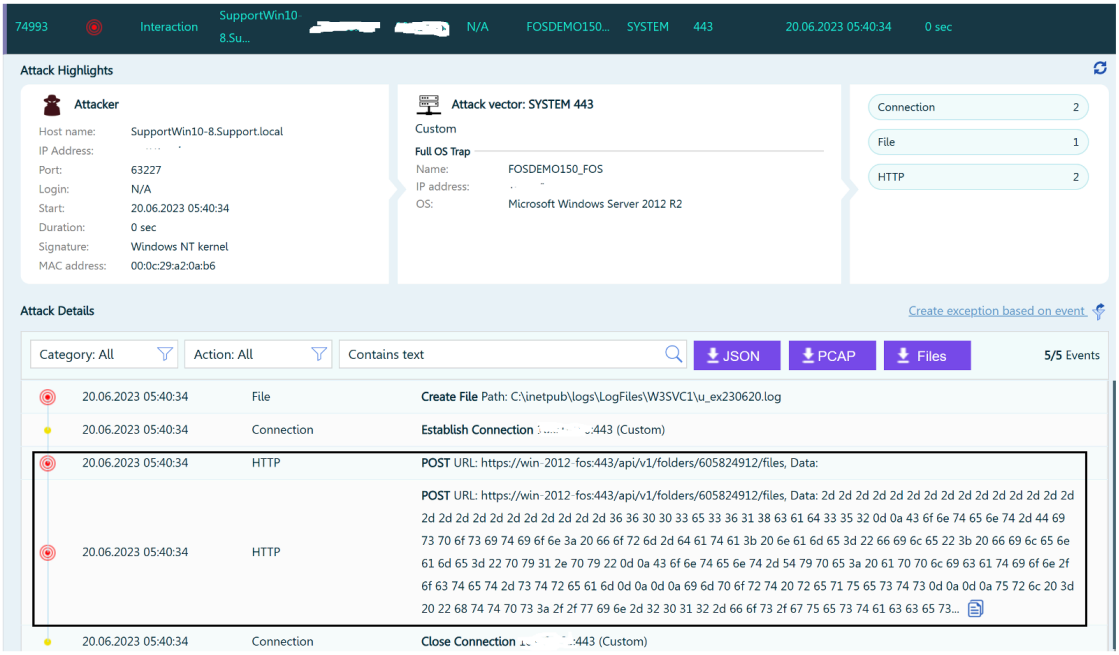

Figure 5: Threatwise detection of the POST command and data uploaded to the decoy

Example C: Related with IIS Event "POST /moveitisapi/moveitisapi.dll action=m2" (see Figure 1, Example C)

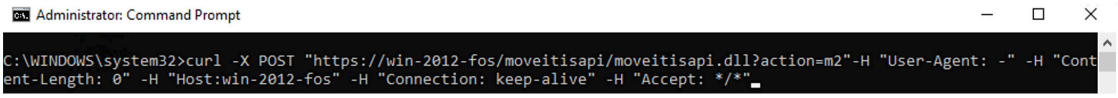

Figure 6: Example C. Sending a POST request to the decoy URL containing movitsapi/moveitsapi.dll results in a similar IIS event as in Figure 1. Example C

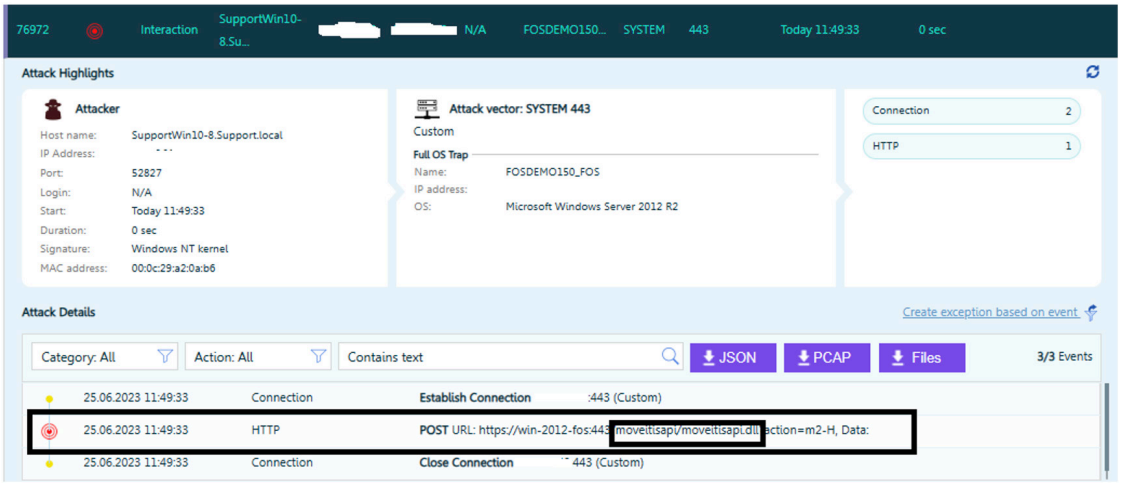

Figure 7: Threatwise detection of POST request sent to the decoy URL, including a clear indication of MOVEit API/dll

Example D: IIS Event:" PUT /api/v1/folders/605824912/files uploadType=resumable&fileId=963061209" (see Figure 1, Example D)

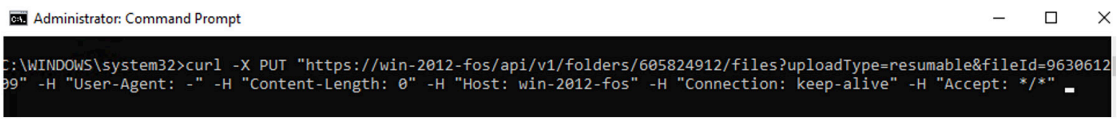

Figure 8: Example D. Sending a PUT request to the decoy URL creating a resource on the server resulting in a similar IIS event as in Figure1, Example D.

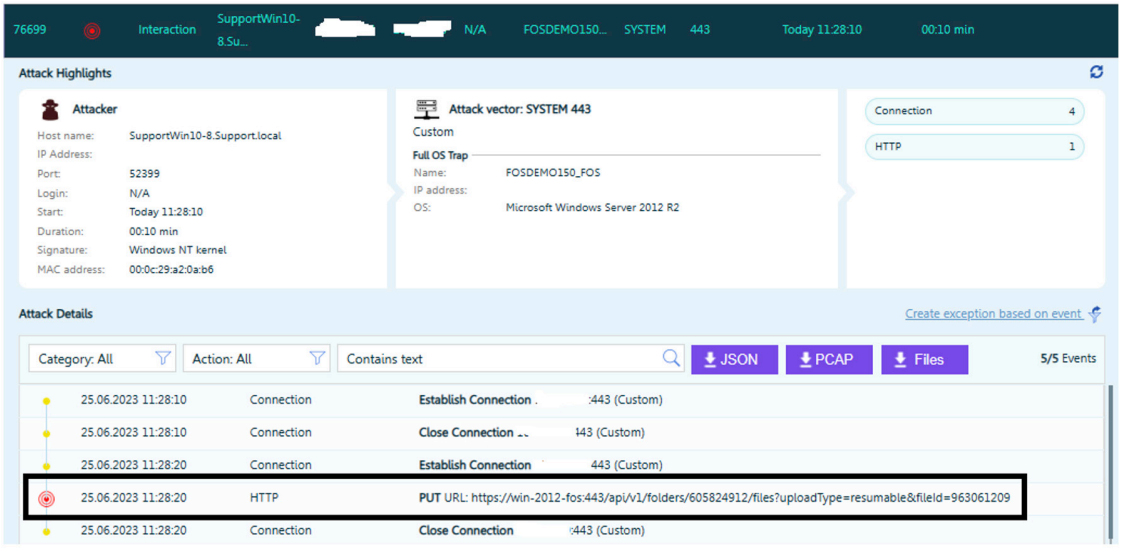

Figure 9: Threatwise detection of the PUT request

SYSAID VULNERABILITY CVE-2023-47246

In a similar incident on November 8, 2023, SysAid reported a vulnerability, now known as CVE-2023-47246. The intruder infiltrated the SysAid Tomcat web service by uploading a malicious WAR archive, including a web shell and other payloads, to the webroot directory at C:\Program Files\SysAidServer\tomcat\webapps\usersfiles. The web shell granted unauthorized access, enabling the attacker to control the system. Using a PowerShell script via the web shell, the attacker executed a malware loader (user.exe), initiating the injection of the GraceWire trojan into processes like spoolsv.exe, msiexec.exe, and svchost.exe. A second PowerShell script was employed to eliminate traces of the attacker's activities from the disk and the SysAid on-prem server web logs.[22] Microsoft threat intelligence determined that the vulnerability was used to deploy CL0P ransomware by a threat actor it tracks as Lace Tempest.[23]

Using Threatwise, customers can create and customize SysAid server decoys, including Tomcat web services, even customized with the same HTML look & feel of SysAid, and collect attempts of intruders uploading WAR archives, web shells, and other payloads to the webroot directory. In addition, on a high interaction Linux decoy running PowerShell scripts, such as executing a malware loader, it will be recorded and trigger an alert in Threatwise.

STRENGTHEN YOUR RESILIENCE AGAINST VULNERABILITY EXPLOITATION WITH THE COMMVAULT CLOUD

1. Surface threats target known vulnerabilities from the moment of their publication instead of waiting for entire patching cycles to be completed.
2. Layer up early warning around critical assets to spot zero-day and silent attacks. Further, harden and protect data in core systems such as active directory (AD).
3. Shield sensitive network segments in production environments, including IoT systems, financial processing segments, operational technology, medical systems, and highly specialized instances.
4. Discover sensitive files and prevent their exfiltration.
5. Isolate malware, remediate risks, and prevent reinfection of your data protected in backup and recovery instances in flight and at rest.
6. Regular cadences analyze, validate, and orchestrate recoveries for a robust cyber recovery plan for ransomware and digital threats.

REFERENCES

1 TechTarget | 10 of the biggest zero-day attacks of 2023 | 2024
2 Darkreading | Cl0P Gang Sat on Exploit for MOVEit Flaw for Nearly 2 Years | 2023
3 BBC | MOVEit hack: BBC, B.A. and Boots among cyber attack victims |2023
4 Bleeping Computers | Clop ransomware claims it breached 130 orgs using GoAnywhere zero-day | 2023
5 Cyber-crime | MOVEit cybercriminals unearth fresh zero-day to exploit on-prem SysAid hosts | 2023
6 Kroll | MOVEit Transfer Vulnerability (CVE-2023-34362 | 2023
7 Bleeping Computers | Clop ransomware claims it breached 130 orgs using GoAnywhere zero-day | 2023
8 Kroll | MOVEit Transfer Vulnerability (CVE-2023-34362 | 2023
9 Kroll | MOVEit Transfer Vulnerability (CVE-2023-34362 | 2023
10 Progress Customer Community | MOVEit Transfer Critical Vulnerability (CVE-2023-34362) | 2023
11 CISA | #StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability | 2023
12 Progress Customer Community | MOVEit Transfer Critical Vulnerability (CVE-2023-35036) | 2023
13 Progress Customer Community | MOVEit Transfer Critical Vulnerability (CVE-2023-35708) | 2023
14 Tech Crunch | US confirms federal agencies hit by MOVEit breach, as hackers list more victims | 2023
15 SC Media | Clop ransomware gang targets SysAid server bug | 2023
16 Silicon Angel | Majority of 2023's critical cyberattacks stemmed from fewer than 1% of vulnerabilities | 2023
17 Mandiant | Zero-Day Vulnerability in MOVEit Transfer Exploited for Data Theft | 2023
18 Horizon | MOVEit Transfer CVE-2023-34362 Deep Dive and Indicators of Compromise | 2023
19 Huntress | MOVEit Transfer Critical Vulnerability CVE-2023-34362 Rapid Response | 2023
20 Huntress | MOVEit Transfer Critical Vulnerability CVE-2023-34362 Rapid Response | 2023
21 Huntress | MOVEit Transfer Critical Vulnerability CVE-2023-34362 Rapid Response | 2023
22 Huntress | Critical Vulnerability: SysAid CVE-2023-47246 | 2023
23 Sysaid | SysAid On-Prem Software CVE-2023-47246 Vulnerability | 2023