



| Flash |

Ransomware Collectives Set to Exploit SysAid Zero-Day Vulnerability

F-2023-11-10a

Classification: TLP:CLEAR

Criticality: High

Intelligence Requirements: Ransomware, Vulnerability Exploitation

November 10, 2023

Scope Note: ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 9:00 AM (EST) on November 10, 2023**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Ransomware Collectives Set to Exploit SysAid Zero-Day Vulnerability

› Key Findings

- On November 8, 2023, IT Service Management Solution (ITSM) organization SysAid disclosed a zero-day vulnerability targeting its on-premises software, which has led to an unknown amount of ransomware attacks.
- Initial exploitation has been attributed to financially-motivated group Lace Tempest, which is associated with ransomware collective C10p. C10p has conducted at least two prominent ransomware campaigns in 2023, both targeting managed file transfer solutions (MFTs).

| Details

On November 8, 2023, ITSM organization SysAid disclosed a zero-day vulnerability (tracked as CVE-2023-47246) targeting its on-premises software, which has led to an unknown amount of ransomware attacks.¹

¹ [hXXps://www.sysaid\[.\]com/blog/service-desk/on-premise-software-security-vulnerability-notification](https://www.sysaid[.]com/blog/service-desk/on-premise-software-security-vulnerability-notification)

- The path traversal vulnerability was reportedly discovered on November 2 by Microsoft Security researchers, prompting the release of a SysAid security patch.²
- The vulnerability is alleged to have been used in the deployment of ransomware, although the extent of the attacks or nature of the victims remain unclear as of the writing of this report.³

The vulnerability enables attackers to upload a WAR archive containing a WebShell into the webroot of the SysAid Tomcat web service, allowing the deployment of a PowerShell Script that executes a malware loader named “user[.]exe” on the compromised host. This injects the GraceWire trojan into various processes (spoolsv[.]exe, msixexec[.]exe, and svchost[.]exe).⁴

- This is followed by human-operated activity, including lateral movement, data theft, and ransomware deployment. Following this intrusion, attackers use a second PowerShell script to wipe evidence of their activity from the disk and the SysAid on-prem server web logs.

The initial exploitation has been attributed to financially-motivated threat group Lace Tempest (also known as DEV-0950), whose activities have displayed overlap with FIN11—notably in their deployment of CI0p ransomware. Typically, CI0p operates with very low levels of activity for several months, followed by several weeks of a high attack tempo.

- This was displayed in 2023 with two prominent campaigns: the targeting of Fortra’s GoAnywhere (CVE-2023-0669) and Progress Software’s MoveIT (CVE-2023-43462) MFT solutions.

² [hXXps://documentation.sysaid\[.\]com/docs/23336](https://documentation.sysaid.com/docs/23336)

³

[hXXps://www.bleepingcomputer\[.\]com/news/security/microsoft-sysaid-zero-day-flaw-exploited-in-ci0p-ransomware-attacks/](https://www.bleepingcomputer.com/news/security/microsoft-sysaid-zero-day-flaw-exploited-in-ci0p-ransomware-attacks/)

⁴ [hXXps://www.sysaid\[.\]com/blog/service-desk/on-premise-software-security-vulnerability-notification](https://www.sysaid.com/blog/service-desk/on-premise-software-security-vulnerability-notification)

- These campaigns were widespread and highly lucrative, accounting for approximately 10 percent of all ransomware and digital extortion (R&DE) attacks observed by ZeroFox Intelligence so far in 2023.⁵⁶⁷

It is likely that CVE-2023-47246 will be exploited in further ransomware attacks against SysAid consumers, which span across at least 140 countries. As well as ClOp, there is a high probability that other ransomware strains will be deployed against unpatched endpoints. However, attacks are unlikely to reach the frequency and magnitude of previous ClOp campaigns.

- The extent of exploitation is dependent on the dispersion of the vulnerability, the extent to which it grants access to sensitive information, and both the efficacy and uptake of SysAid security patches, among other factors.

⁵ ZeroFox Internal Intelligence Collections

⁶ [hXXps://cyberint\[.\]com/blog/research/moveit-supply-chain-attack/](https://cyberint[.]com/blog/research/moveit-supply-chain-attack/)

⁷ [hXXps://www.securityweek\[.\]com/goanywhere-zero-day-attack-hits-major-orgs/](https://www.securityweek[.]com/goanywhere-zero-day-attack-hits-major-orgs/)

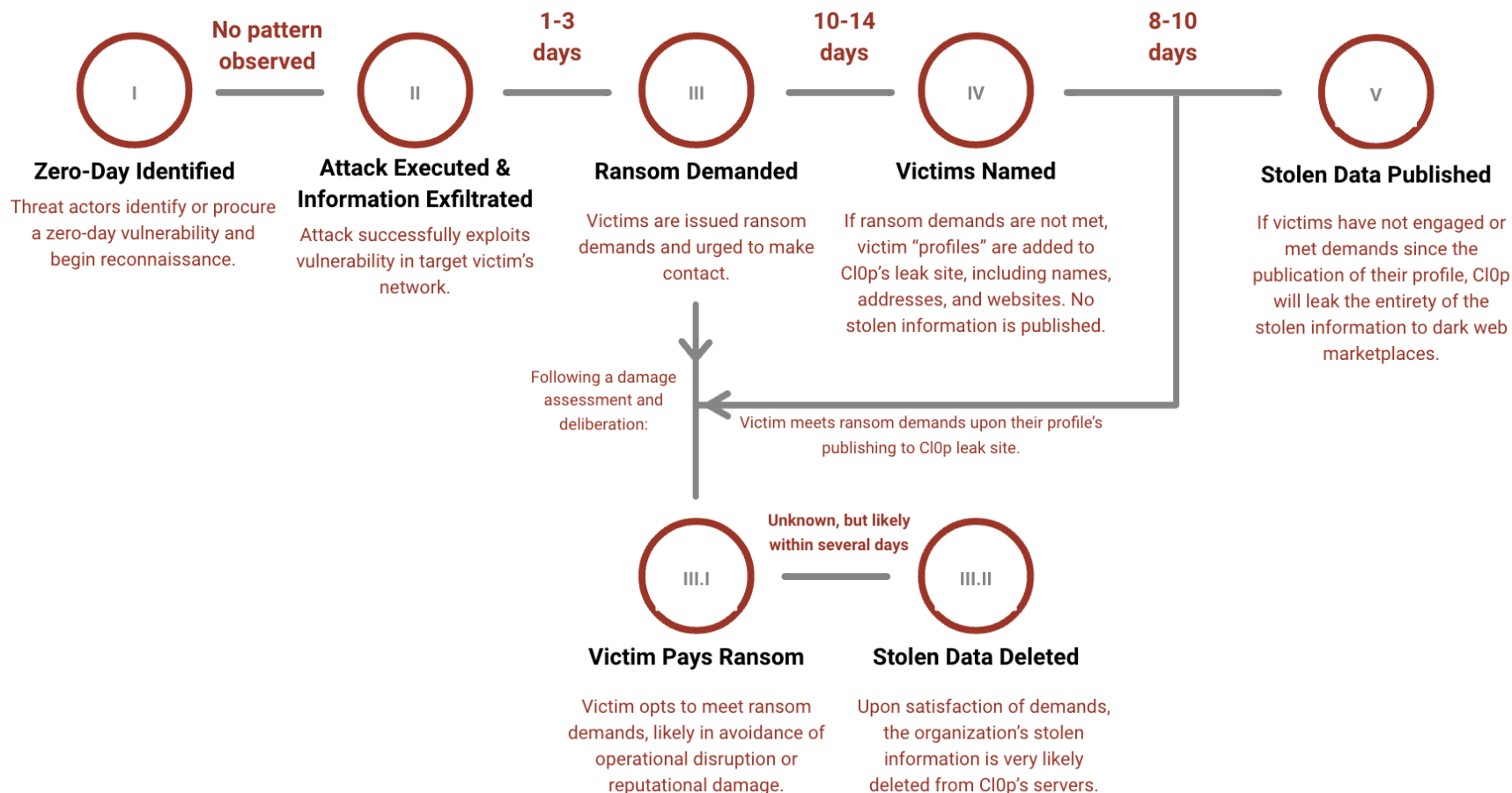
Flash | Ransomware Collectives Set to Exploit SysAid Zero-Day Vulnerability

F-2023-11-10a
TLP: CLEAR



Typical Timescale for CI0p's Extortion*

*Medium confidence assessment based on observed procedures and timeframes



Source: ZeroFox Intelligence

Flash | Ransomware Collectives Set to Exploit SysAid Zero-Day Vulnerability

F-2023-11-10a

TLP: CLEAR

Recommendations

- Ensure SysAid systems are updated to version 23.3.36, which includes patches for the identified vulnerability.
- Conduct a thorough assessment of your SysAid server to look for any indicators of compromise (IOCs), and review any relevant activity logs for suspicious behavior.
- Delete any unauthorized files and user accounts.
- Reset account credentials for affected systems.
- Utilize the ZeroFox Platform to perform searches on relevant IOCs and further developments.

Flash | Ransomware Collectives Set to Exploit SysAid Zero-Day Vulnerability

F-2023-11-10a

TLP:CLEAR

Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

Flash | Ransomware Collectives Set to Exploit SysAid Zero-Day Vulnerability

F-2023-11-10a

TLP: CLEAR

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%