

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Lace Tempest Exploits Zero-Day in a Strategic Strike on SysAid

Date of Publication

November 10, 2023

Admiralty Code

A1

TA Number

TA2023457

Summary

First Seen: November 2, 2023

Threat Actor: Lace Tempest (aka DEV-0950, FIN11)




Malware: Clop ransomware, Gracewire (FlawedGrace)

Affected Product: SysAid servers

Vulnerable Industries: Automation, Healthcare, Human Resources, Higher Education, and Manufacturing

Impact: Lace Tempest has been implicated in exploiting a zero-day vulnerability, identified as CVE-2023-47246. This exploitation allows for the execution of code within SysAid on-premise software, leading to an unauthorized breach of corporate servers. The primary objectives of this breach include data theft and the deployment of the Clop ransomware.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-47246	SysAid path traversal vulnerability	SysAid: 21.4.45 - 23.3.35			

Vulnerability Details

#1

The threat actor, known as Lace Tempest (also referred to as FIN11), has been linked to the exploitation of a zero-day vulnerability identified as CVE-2023-47246. This exploit enables the execution of code within the SysAid on-premise software, providing unauthorized access to corporate servers. The main objectives of this infiltration encompass data theft and the deployment of the notorious Clop ransomware, recognized for exploiting zero-day vulnerabilities in widely used software. Notably, Lace Tempest is the same threat actor responsible for the [MOVEit Transfer](#) and [GoAnywhere MFT](#) extortion attacks earlier this year.

#2

The attacker uploaded a Web Archive (WAR) containing a WebShell and additional payloads to the webroot of the SysAid Tomcat web service. The WebShell, in turn, granted the attacker unauthorized access, facilitating the delivery of a PowerShell script designed to execute a loader responsible for deploying the Gracewire trojan.

#3

Following the initial compromise, the attacker systematically removes the payloads used to establish an initial foothold on the compromised servers. Furthermore, the attack sequences are distinguishable by the use of the MeshCentral Agent and PowerShell to download and execute Cobalt Strike, a legitimate post-exploitation framework.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-47246	SysAid: 21.4.45 - 23.3.35	cpe:2.3:a:sysaid:sysaid:- :*:*:*:*:*:*	CWE-22

Recommendations



Prioritize Patching: It is strongly recommended that organizations with on-premise SysAid servers promptly apply the vendor-supplied [patches](#) available in version 23.3.36. Given the potential risks associated with ransomware and extortion attacks, this action should be treated as an emergency measure. Organizations are also encouraged to activate incident response procedures where applicable and to ensure that the SysAid server is not exposed to the public internet.



SysAid Tomcat Webroot Analysis: Regularly inspect the SysAid Tomcat webroot for the presence of unusual files, paying specific attention to WAR, ZIP, or JSP files with atypical timestamps. Conduct thorough scans for unauthorized WebShell files within the SysAid Tomcat service. Scrutinize JSP files for potential malicious content that may indicate a security compromise.



Process Monitoring: Monitor system logs for unexpected child processes originating from Wrapper.exe, which could be indicative of WebShell usage. Regularly review PowerShell logs for script executions aligning with known attack patterns associated with the identified vulnerability. Keep a vigilant eye on key processes such as spoolsv.exe, msixexec.exe, and svchost.exe for any signs of unauthorized code injection.

Potential MITRE ATT&CK TTPs

<u>TA0042</u> Resource Development	<u>TA0002</u> Execution	<u>TA0003</u> Persistence	<u>TA0005</u> Defense Evasion
<u>TA0007</u> Discovery	<u>TA0008</u> Lateral Movement	<u>TA0009</u> Collection	<u>TA0010</u> Exfiltration
<u>TA0011</u> Command and Control	<u>T1588.006</u> Vulnerabilities	<u>T1588</u> Obtain Capabilities	<u>T1059.001</u> PowerShell
<u>T1543</u> Create or Modify System Process	<u>T1505</u> Server Software Component	<u>T1564</u> Hide Artifacts	<u>T1059</u> Command and Scripting Interpreter
<u>T1083</u> File and Directory Discovery	<u>T1046</u> Network Service Discovery	<u>T1057</u> Process Discovery	<u>T1070</u> Indicator Removal
<u>T1570</u> Lateral Tool Transfer	<u>T1213</u> Data from Information Repositories	<u>T1105</u> Ingress Tool Transfer	<u>T1041</u> Exfiltration Over C2 Channel

🔗 Indicators of Compromise (IOCs)

TYPE	VALUE
File Name	user.exe
SHA256	b5acf14cdac40be590318dee95425d0746e85b1b7b1cbd14da66f21f2522bf4d
IPv4	81.19.138[.]52, 45.182.189[.]100, 179.60.150[.]34, 45.155.37[.]105
File Paths	C:\Program Files\SysAidServer\tomcat\webapps\usersfiles\user.exe, C:\Program Files\SysAidServer\tomcat\webapps\usersfiles.war, C:\Program Files\SysAidServer\tomcat\webapps\leave

🔗 Patch Details

All users of SysAid are strongly encouraged to transition to version 23.3.36 or a subsequent release.

Link:

<https://documentation.sysaid.com/docs/latest-version-installation-files>

🔗 References

<https://www.sysaid.com/blog/service-desk/on-premise-software-security-vulnerability-notification>

<https://www.rapid7.com/blog/post/2023/11/09/etr-cve-2023-47246-sysaid-zero-day-vulnerability-exploited-by-lace-tempest/>

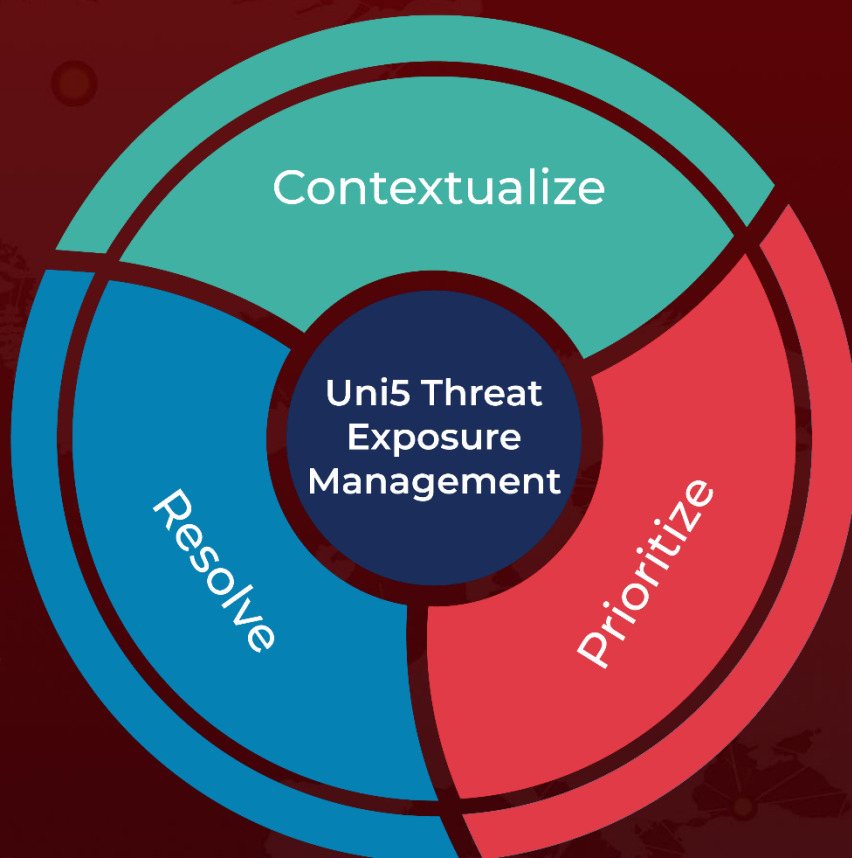
<https://www.hivepro.com/threat-advisory/clop-ransomware-group-claims-responsibility-for-goanywhere-mft-attacks/>

<https://www.hivepro.com/threat-advisory/the-exploitation-of-critical-zero-day-vulnerability-found-in-moveit-transfer/>

What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

November 10, 2023 • 4:30 AM

© 2023 All Rights are Reserved by Hive Pro®



More at www.hivepro.com