aDvens

Security for the greater good

Bulletin d'alerte
Vulnérabilité critique dans Atlassian Confluence

2023-11-07 | **TLP:CLEAR** | CERT aDvens - CTI
Advens - 16 Quai de la Mégisserie - 75001 Paris

Sommaire

CVE-2023-22518

Le 31 octobre 2023, Atlassian a publié un bulletin de sécurité indiquant la découverte d'une nouvelle vulnérabilité critique dans Confluence Data Center et Server. Cette faille provient d'un défaut de contrôle des droits dans le module *WebSudo*.

En envoyant des requêtes spécifiquement forgées, un attaquant distant et non authentifié peut exécuter des commandes arbitraires sur le serveur.

Cette vulnérabilité est actuellement exploitée pour déployer le ransomware Cerber.

Type de vulnérabilité

- **CWE-285** : Improper Authorization

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	Aucun
Privilèges requis	Aucun	Impact sur l'intégrité	Élevé
Interaction de l'utilisateur	Aucune	Impact sur la disponibilité	Élevé

Produits impactés

- Atlassian Confluence Data Center et Server

Recommandations

Le CERT aDvens recommande de tester les mesures de contournement proposées dans un environnement dédié avant leur déploiement en production afin de prévenir tout effet de bord.

- Mettre à jour Atlassian Confluence Data Center et Server versions 7.19.x et antérieures vers la version 7.19.16.
- Mettre à jour Atlassian Confluence Data Center et Server versions 7.20.x et ultérieures vers la version 8.3.4, 8.4.4, 8.5.3 ou 8.6.1.

Si le correctif ne peut pas être déployé, il est recommandé de désactiver l'accès aux ressources :

- /json/setup-restore.action
- /json/setup-restore-local.action
- /json/setup-restore-progress.action

Des informations complémentaires sont disponibles dans le bulletin d'Atlassian.

Preuve de concept

Une preuve de concept est disponible en source ouverte.

Indicateurs de Compromissions

TLP	TYPE	VALEUR
TLP:CLEAR	IP	193.176.179.41
TLP:CLEAR	IP	193.43.72.11
TLP:CLEAR	IP	45.145.6.112
TLP:CLEAR	Domaine	j3qxmk6g5sk3zw62i2yhjnwmhm55rfz47fdyfkhaithlpelfjdokdxad[.]onion
TLP:CLEAR	MD5 I Artefact	81b760d4057c7c704f18c3f6b3e6b2c4 I /tmp/agttydcb.bat
TLP:CLEAR	SHA256 I Artefact	4ed46b98d047f5ed26553c6f4fded7209933ca9632b998d265870e3557a5cdfe I /tmp/qnetd

Références

- https://nvd.nist.gov/vuln/detail/CVE-2023-22518
- https://confluence.atlassian.com/security/cve-2023-22518-improper-authorization-vulnerability-in-confluence-data-center-and-server-1311473907.html
- https://jira.atlassian.com/browse/CONFSERVER-93142
- https://www.bleepingcomputer.com/news/security/critical-atlassian-confluence-bug-exploited-in-cerber-ransomware-attacks/