aDvens

Security for the greater good

Bulletin d’alerte
Vulnérabilité critique dans Qlik

2023-12-04 | **TLP:CLEAR** | CERT aDvens - CTI

Advens - 16 Quai de la Mégisserie - 75001 Paris

Sommaire

Qlik

Le 29 août 2023, Qlik a publié un bulletin de sécurité dans lequel l'éditeur annonce la découverte de deux vulnérabilités : CVE-2023-41266 et CVE-2023-41265.

Le 20 septembre 2023, Qlik alerte dans un nouveau bulletin de la correction partielle de la CVE-2023-41265 et de la découverte d'une nouvelle vulnérabilité (CVE-2023-48365).

Qlik Sense est une plateforme Cloud d'analyse et de visualisation de données.

Ces trois vulnérabilités sont activement exploitées par le groupe de ransomware Cactus.

CVE-2023-41266

Un défaut de contrôle des données fournies par l'utilisateur, permet à un attaquant distant et non authentifié, de générer une session anonyme lui permettant d'effectuer des requêtes HTTP vers des points d'accès non autorisés.

Type de vulnérabilité

- CWE-20 : Improper Input Validation

Risque

- Contournement de la politique de sécurité

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	Faible
Interaction de l'utilisateur	Aucune	Impact sur la disponibilité	Aucun

Produits impactés

Versions Qlik Sense Entreprise pour environnement Windows :

- August 2022 Patch 12 et antérieures
- November 2022 Patch 10 et antérieures
- February 2023 Patch 7 et antérieures
- May 2023 Patch 3 et antérieures

Preuve de concept

Une preuve de concept est disponible en sources ouvertes.

CVE-2023-41265

Un défaut de contrôle de requêtes HTTP permet à un attaquant authentifié, en envoyant des requêtes spécifiquement forgées, de communiquer avec les serveurs applicatifs (Backend) et d'élever ses privilèges.

L'exploitation conjointe des vulnérabilités CVE-2023-41265 et CVE-2023-41266 permettrait à un attaquant, distant et non authentifié, d'exécuter du code à distance.

Type de vulnérabilité

- CWE-444 : Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')

Risques

- Contournement de la politique de sécurité
- Élévation de privilèges
- Exécution de code arbitraire

Criticité (score de base CVSS v3.1)

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

Produits impactés

Versions Qlik Sense Entreprise pour environnement Windows :

- August 2022 Patch 12 et antérieures
- November 2022 Patch 10 et antérieures
- February 2023 Patch 7 et antérieures
- May 2023 Patch 3 et antérieures

Preuve de concept

Une preuve de concept est disponible en sources ouvertes.

CVE-2023-48365

Un défaut de contrôle de requêtes HTTP dans *Qlik Sense Entreprise* permet à un attaquant distant, via des requêtes spécifiquement forgées, d'exécuter du code arbitraire sur le système avec des droits privilégiés.

Type de vulnérabilité

- CWE-444 : Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')

Risques

- Elévation de privilèges
- Exécution de code arbitraire

Criticité (score de base CVSS v3.1)

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

Produits impactés

Versions Qlik Sense Entreprise pour environnement Windows :

- November 2021 Patch 16 et antérieures
- February 2022 Patch 14 et antérieures
- May 2022 Patch 15 et antérieures
- August 2022 Patch 13 et antérieures
- November 2022 Patch 11 et antérieures
- February 2023 Patch 9 et antérieures
- May 2023 Patch 5 et antérieures
- August 2023 Patch 1

Recommandations

- Appliquer le Correctif Patch 17 à Qlik Sense Entreprise pour Windows version November 2021.
- Appliquer le Correctif Patch 15 à Qlik Sense Entreprise pour Windows version February 2022.
- Appliquer le Correctif Patch 16 à Qlik Sense Entreprise pour Windows version May 2022.
- Appliquer le Correctif Patch 14 à Qlik Sense Entreprise pour Windows version August 2022.
- Appliquer le Correctif Patch 12 à Qlik Sense Entreprise pour Windows version November 2022.
- Appliquer le Correctif Patch 10 à Qlik Sense Entreprise pour Windows version February 2023.
- Appliquer le Correctif Patch 6 à Qlik Sense Entreprise pour Windows version May 2023.
- Appliquer le Correctif Patch 2 à Qlik Sense Entreprise pour Windows version August 2023.

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

Preuve de concept

Une preuve de concept est disponible en sources ouvertes.

Indicateurs de Compromission

TLP	TYPE	VALEUR	COMMENTAIRE
TLP:CLEAR	IP	45.61.147[.]176	ManageEngine Server IP for zohoservice[.]net
TLP:CLEAR	IP	216.107.136[.]46	ManageEngine Server Hosting payload over HTTP
TLP:CLEAR	IP	144.172.122[.]30	ManageEngine Server Hosting payload over HTTP
TLP:CLEAR	Domain	zohoservice[.]net	Hosting payload over HTTP
TLP:CLEAR	URL	http[:]//zohoservice[.]net/putty.zip	Renamed PuTTY Link (Plink)
TLP:CLEAR	URL	http[:]//216.107.136[.]46/Qliksens_update.zip	Renamed ManageEngine UEMS
TLP:CLEAR	URL	http[:]//216.107.136[.]46/Qliksens_updated.zip	Renamed ManageEngine UEMS
TLP:CLEAR	URL	http[:]//zohoservice[.]net/qlik-sens-Patch.zip	Renamed ManageEngine UEMS
TLP:CLEAR	URL	http[:]//zohoservice[.]net/qlik-sens-nov.zip	Renamed ManageEngine UEMS
TLP:CLEAR	File Path	C:\Users\Public\svchost.exe	Renamed Rclone
TLP:CLEAR	File Path	c:\windows\temp\file.exe	Renamed AnyDesk
TLP:CLEAR	File Path	c:\windows\temp\putty.exe	Renamed PuTTY Link (Plink)
TLP:CLEAR	File Path	c:\windows\temp\Qliksens.exe	Renamed ManageEngine UEMS
TLP:CLEAR	File Path	c:\windows\temp\any.exe	Renamed ManageEngine UEMS
TLP:CLEAR	File Path	C:\temp\putty.exe	Renamed PuTTY Link (Plink)
TLP:CLEAR	File Path	C:\Windows\appcompat\AcRes.exe	Renamed ManageEngine UEMS
TLP:CLEAR	Filename	file.exe	Renamed AnyDesk Installer
TLP:CLEAR	Filename	anydesk.zip	Renamed AnyDesk Installer
TLP:CLEAR	Filename	AcRes.exe	Renamed ManageEngine UEMS
TLP:CLEAR	Filename	any.exe	Renamed AnyDesk Installer
TLP:CLEAR	Filename	putty.zip	ZIP containing PuTTY Link (Plink)
TLP:CLEAR	Filename	Qlik_sense_enterprise.zip	Renamed ManageEngine UEMS
TLP:CLEAR	Filename	qlik-sens-nov.zip	Renamed ManageEngine UEMS
TLP:CLEAR	Filename	qlik-sens-Patch.zip	Renamed ManageEngine UEMS
TLP:CLEAR	Filename	Qliksens.exe	Renamed ManageEngine UEMS
TLP:CLEAR	Filename	Qliksens_updated.zip	Renamed ManageEngine UEMS
TLP:CLEAR	Filename	Qliksens_update.zip	Renamed ManageEngine UEMS

TLP	TYPE	VALEUR	COMMENTAIRE
TLP:CLEAR	SHA256	828e81aa16b2851561fff6d3127663ea2d1d68571f06cbd732fdf5672086924d	PuTTY Link (Plink)
TLP:CLEAR	SHA256	90b009b15eb1b5bc4a990ecdd86375fa25eaa67a8515ae6c6b3b58815d46fa82	ManageEngine UEMS Installer
TLP:CLEAR	SHA256	3ac8308a7378dfe047eacd393c861d32df34bb47535972eb0a35631ab964d14d	ManageEngine UEMS Installer
TLP:CLEAR	SHA256	6cb87cad36f56aefcefbe754605c00ac92e640857fd7ca5faab7b9542ef80c96	ManageEngine UEMS Installer

Références

- https://arcticwolf.com/resources/blog/qlik-sense-exploited-in-cactus-ransomware-campaign/
- https://community.qlik.com/t5/Support-Updates/Qlik-Sense-Enterprise-for-Windows-New-Security-Patches-Available/ba-p/2108549
- https://community.qlik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/ta-p/2110801
- https://community.qlik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/tac-p/2120510
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-48365
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-41266
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-41265