aDvens

Security for the greater good

Bulletin d'alerte
Vulnérabilités critiques dans ScreenConnect

2024-02-22 | **TLP:CLEAR** | CERT aDvens - CTI
Advens - 16 Quai de la Mégisserie - 75001 Paris

aDvens

Sommaire

ConnectWise ScreenConnect

Le 19 février 2024, ConnectWise a publié un correctif de sécurité pour leur outil d'accès à distance ScreenConnect. Cette publication fait suite au signalement de deux vulnérabilités le 13 février 2024 via leur plateforme Connectwise Trust Center. Aucun ID de CVE n'a été assigné.

Mise à jour du 22 février 2024 : Le CISA a attribué les identifiants CVE-2024-1708 et CVE-2024-1709 pour ces deux vulnérabilités affectant *ConnectWise ScreenConnect*. ConnectWise a également modifié les recommandations de mise à jour de son bulletin le 21 février 2024 et a retiré les restrictions de licence pour les produits qui ne seraient plus sous support.

CVE-2024-1709

Un défaut de contrôle d'accès permet à un attaquant non authentifié d'accéder à l'assistant d'installation de ScreenConnect normalement restreint aux utilisateurs authentifiés. Cet accès lui permet de créer un compte administrateur et d'accéder à des données confidentielles. L'exploitation de cette vulnérabilité est peu complexe.

Cette vulnérabilité est actuellement exploitée

Type de vulnérabilité

- **CWE-288** : Authentication bypass using an alternate path or channel

Risques

- Contournement d'authentification
- Atteinte à la confidentialité des données

Criticité (Score de base CVSS v3.1)

Vecteur d'attaque	Réseau	Portée	Changée
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

- ConnectWise ScreenConnect versions 23.9.7 et antérieures

Recommandations

- Mettre à jour ConnectWise ScreenConnect vers la version 23.9.8 pour les installations on-premise et auto-hébergées.
- Des informations complémentaires sont disponibles dans le bulletin de sécurité ConnectWise.

Mise à jour du 22 février 2024 : ConnectWise met à disposition une version (23.9.10.8817) comprenant des correctifs pour améliorer l'expérience client en complément de la correction des vulnérabilités. Dans cette dernière version, les restrictions de licence ont été retirées pour corriger les produits ne disposant plus de support.

Preuve de concept

Une preuve de concept est disponible en sources ouvertes.

Détection

- L'exploitation de la vulnérabilité implique une modification du fichier **C:\Program Files (x86)\ScreenConnect\AppData\User.xml**. Ce fichier contient les utilisateurs créés et les informations de dernière connexion. La présence d'un nouvel utilisateur et sa connexion récente pourraient indiquer une compromission.
- La mise en place d'une stratégie d'audit de sécurité avancée pour journaliser les événements 4663 et la configuration d'une liste de contrôle d'accès système (SACL) sur le répertoire **C:\Windows\Temp\ScreenConnect\<ScreenConnectVersion>** permet de détecter une activité de modification du fichier cité supra.

Sigma

```
title: ConnectWise ScreenConnect SetupWizard Authentication Bypass (Feb 2024)
id: d27eabad-9068-401a-b0d6-9eac744d6e67
status: experimental
description: Detects http requests to '/SetupWizard.aspx/' that indicate exploitation of the ScreenConnect
vulnerability.
references:
  - https://www.connectwise.com/company/trust/security-bulletins/connectwise-screenconnect-23.9.8
  - https://www.huntress.com/blog/vulnerability-reproduced-immediately-patch-screenconnect-23-9-8
  - https://www.huntress.com/blog/detection-guidance-for-connectwise-cwe-288-2
author: Huntress DE&TH Team
date: 2024/02/20
logsource:
  category: webserver
  product: windows
detection:
    selection:
      cs-uri-query|contains: '/SetupWizard.aspx/'
    condition: selection
falsepositives:
    - Unknown
level: critical
tags:
  - attack.initial_access
  - attack.persistence
```

```
title: ConnectWise ScreenConnect SetupWizard User Database Modification
id: 4109cb6a-a4af-438a-9f0c-056abba41c6f
status: experimental
description: This detects file modifications to the temporary xml user database file indicating local user
modification in the ScreenConnect server. This will occur during exploitation of the ScreenConnect
Authentication Bypass vulnerability in versions <23.9.8, but may also be observed when making legitimate
modifications to local users or permissions. This requires an Advanced Auditing policy to log a successful
Windows Event ID 4663 events and with a SACL set on the directory.
references:
    - https://www.connectwise.com/company/trust/security-bulletins/connectwise-screenconnect-23.9.8
    - https://www.huntress.com/blog/vulnerability-reproduced-immediately-patch-screenconnect-23-9-8
    - https://www.huntress.com/blog/detection-guidance-for-connectwise-cwe-288-2
author: Huntress DE&TH Team
date: 2024/02/20
logsource:
    product: windows
    service: security
detection:
    selection:
        EventID: 4663
        ObjectType: 'File'
        ProcessName|contains:
            - 'ScreenConnect.Service.exe'
        AccessMask: 0x6
        ObjectName|endswith: '.xml'
        ObjectName|contains|all:
            - 'Temp'
            - 'ScreenConnect'
    condition: selection
falsepositives:
    - Unknown
level: critical
tags:
  - attack.initial_access
  - attack.persistence
```

Yara

```
rule ConnectWise_ScreenConnect_Authentication_Bypass_Feb_2024_Exploitation_IIS_Logs {
   meta:
      description = "Detects an http request to '/SetupWizard.aspx/' with anything following it, which when
found in IIS logs is a potential indicator of compromise of the 2024 ConnectWise ScreenConnect (versions
prior to 23.9.8) vulnerability that allows an Authentication Bypass"
      author = "Huntress DE&TH Team"
      reference = "https://www.connectwise.com/company/trust/security-bulletins/connectwise-screenconnect-
23.9.8"
      date = "2024-02-20"
      id = "2886530b-e164-4c4b-b01e-950e3c40acb4"
   strings:
      $s1 = "/SetupWizard.aspx/" ascii
   condition:
      $s1
}
```

CVE-2024-1708

Cette vulnérabilité de type Path Traversal permet à un attaquant avec des privilèges élevés de mener une attaque Zip Slip et d'exécuter du code arbitraire à distance. L'obtention des privilèges peut s'effectuer via l'exploitation de la première vulnérabilité.

Type de vulnérabilité

- **CWE-22** : Improper limitation of a pathname to a restricted directory ("path traversal")

Risque

- 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	Élevé	Impact sur l'intégrité	Élevé
Interaction de l'utilisateur	Requise	Impact sur la disponibilité	Élevé

Produits impactés

- ConnectWise ScreenConnect versions 23.9.7 et antérieures

Recommandations

- Mettre à jour ConnectWise ScreenConnect vers la version 23.9.8 pour les installations on-premise et auto-hébergées.
- Des informations complémentaires sont disponibles dans le bulletin de sécurité ConnectWise.

Mise à jour du 22 février 2024 : ConnectWise met à disposition une version (23.9.10.8817) comprenant des correctifs pour améliorer l'expérience client en complément de la correction des vulnérabilités. Dans cette dernière version, les restrictions de licence ont été retirées pour corriger les produits ne disposant plus de support.

Preuve de concept

Une preuve de concept est disponible en sources ouvertes.

Détection

- La mise en place d'une stratégie d'audit de sécurité avancée pour journaliser les événements 4663 et la configuration d'une liste de contrôle d'accès système (SACL) sur le répertoire **C:\Program Files (x86)\ScreenConnect\App_Extensions** permet de détecter l'écriture de fichiers **.aspx** et **.ashx** correspondant à du code malveillant. ScreenConnect n'écrit pas de fichiers dans ce répertoire.

Sigma

```
title: ConnectWise ScreenConnect ZipSlip Exploitation (Feb 2024)
id: 4c198a60-7d05-4daf-8bf7-4136fb6f5c62
status: experimental
description: This detects file modifications to ASPX and ASHX files within the root of the App_Extensions
directory, which is allowed by a ZipSlip vulnerability in versions prior to 23.9.8.  This does occur during
exploitation of the vulnerability. This requires an Advanced Auditing policy to log a successful Windows
Event ID 4663 events and with a SACL set on the directory.
references:
  - https://www.connectwise.com/company/trust/security-bulletins/connectwise-screenconnect-23.9.8
  - https://www.huntress.com/blog/vulnerability-reproduced-immediately-patch-screenconnect-23-9-8
  - https://www.huntress.com/blog/detection-guidance-for-connectwise-cwe-288-2
author: Huntress DE&TH Team
date: 2024/02/20
logsource:
  product: windows
  service: security
detection:
  selection:
    EventID: 4663
    ObjectType: 'File'
    ProcessName|contains:
      - 'ScreenConnect.Service.exe'
    AccessMask: 0x6
  legitimate_path:
    ObjectName|endswith: 'ScreenConnect\App_Extensions\*\*'
  illegitimate_path:
    ObjectName|endswith: 'ScreenConnect\App_Extensions\*.as?x'
  condition: selection and illegitimate_path and not legitimate_path
falsepositives:
  - Unknown
level: critical
tags:
  - attack.initial_access
  - attack.persistence
```

Références

- https://www.connectwise.com/company/trust/security-bulletins/connectwise-screenconnect-23.9.8
- https://www.huntress.com/blog/detection-guidance-for-connectwise-cwe-288-2
- https://www.cve.org/CVERecord?id=CVE-2024-1709
- https://www.cve.org/CVERecord?id=CVE-2024-1708