cyberelements Gate

cyberelements Cleanroom

# Installation du Patch LastDisco

WWW.systancia.com

| | |
|---|---|
| **Réf. :** | Installation du Patch LastDisco |
| **Version :** | 1.01 |
| **Produit :** | **cyber**elements Gate & Cleanroom |
| **Date :** | 2026-07-27 |

**Objet :**

Ce document décrit l'installation du patch de sécurité LastDisco pour cyberelements Gate et Cleanroom sur les différents serveurs applicables

TABLE DES MATIERES

1 Introduction ..... 4
1.1 Public cible ..... 4
1.2 Compatibilité ..... 4
2 Déroulement de l'application du patch de sécurité ..... 5
3 Application du patch de sécurité ..... 6
4 Vérification de l'application du patch de sécurité ..... 7

# 1 Introduction

Ce document détaille la procédure visant à appliquer le patch de sécurité pour la faille LastDisco sur les serveurs **cyber**elements Gate et Cleanroom OnPremise compatibles.

Les environnements SaaS (cyberelements.io, Workroom Session Service et Cleanroom Session Service) ont d'ores et déjà été patchés.

## 1.1 Public cible

| Public cible | | Commentaires |
|---|---|---|
| **Tout public** | ✗ | |
| **Partenaires/intégrateurs** | ✓ | Un accès SSH et les droits root sur l'ensemble des Mediation Controller sont requis. |
| **Utilisateurs finaux** | ✗ | |
| **Administrateurs** | ✓ | Un accès SSH et les droits root sur l'ensemble des Mediation Controller sont requis. |

## 1.2 Compatibilité

Le patch de sécurité s'applique à :

- Tous serveurs Mediation Controller (architecture Standalone ou Cluster) à partir de la version 8.1 de **cyber**elements Gate.
- Tous serveurs Mediation Controller (architecture Standalone ou Cluster) à partir de la version 4.4 de **cyber**elements Cleanroom.

# 2 Déroulement de l'application du patch de sécurité

Avant d'appliquer le patch de sécurité sur les serveurs compatibles, veiller à réaliser les actions suivantes :

1. Réaliser une sauvegarde ou un snapshot des machines sur lesquelles le patch de sécurité sera appliqué.
2. Prévoir un temps de maintenance de la plateforme de 5 minutes par machine sur laquelle le patch de sécurité sera appliqué.

L'application du patch de sécurité peut être parallélisée sur l'ensemble des machines concernées, aucun redémarrage de ces machines ne sera requis après l'application du patch de sécurité.

Avant de démarrer l'application du patch de sécurité, prévoyez les éléments suivants :

- Un outil de transfert de fichiers SFTP (sous Windows WinSCP ou FileZilla peuvent être utilisés).
- Un outil de connexion SSH (sous Windows PuTTY peut être utilisé).
- Les informations de connexion aux différents serveurs avec un compte utilisateur standard et root.
- Le script SH permettant le déploiement du patch de sécurité.

# 3 Application du patch de sécurité

Sur les différents serveurs applicables, envoyer le fichier `IPD-57082.sh` dans le répertoire `/tmp/` à l'aide d'un outil de transfert de fichiers SFTP.

**Cas particulier de l'utilisation du serveur d'intégrité** : si un tel serveur a été déployé, le passer en mode permissif avant application du patch de sécurité. Pour ce faire, se connecter en SSH sur le serveur d'intégrité et exécuter la commande suivante en tant que root :

```
1 #   /usr/local/ipdiva/iis/bin/ipdivaiisctrl.py enablepermissive
```

Se connecter en SSH sur les serveurs sur lesquels le patch de sécurité doit être appliqué et passer en tant que root. Lancer l'application du patch de sécurité avec la commande suivante :

```
1 #   bash /tmp/IPD-57082.sh
```

À noter que lors de l'application du patch de sécurité, un contrôle d'intégrité du script est réalisé pour assurer la bonne application du patch de sécurité.

Si l'application du patch de sécurité a réussi, les messages suivants apparaîtront :

```
SUCCESS: IPD-57074 applied
[…]
SUCCESS: /disconnect fixed: Anonymous grants 89 -> 0, now acquires every
permission
SUCCESS: IPD-57082 run successfully
```

Si le patch de sécurité a déjà été appliqué, le message suivant apparaîtra :

```
INFO: /disconnect: nothing to fix (already acquires every permission, no local
Anonymous grant)
```

Si l'application du patch de sécurité a échoué, récupérer les informations affichées lors de son application pour les transmettre au Support Systancia puis revenir sur la sauvegarde ou le snapshot réalisé avant application du patch de sécurité.

**Cas particulier de l'utilisation du serveur d'intégrité** : en raison de la modification des composants côté Mediation Controller, un nouveau calcul des hash des composants doit être réalisé, puis le mode permissif peut être désactivé. Pour ce faire, se connecter en SSH sur le serveur d'intégrité et exécuter les commandes suivantes en tant que root :

```
1 #   /usr/local/ipdiva/iis/bin/ipdivaiisctrl.py updatehashes
2 #   /usr/local/ipdiva/iis/bin/ipdivaiisctrl.py disablepermissive
```

Arrivé à cette étape, l'application du patch de sécurité est terminée.

# 4 Vérification de l'application du patch de sécurité

Une fois le patch de sécurité déployé sur l'ensemble des serveurs de Mediation Controller, il est possible de vérifier que la plateforme n'est plus vulnérable avec la commande suivante :

```
1 #   MEDIATION=mediation.example.com bash -c "code=\$(curl -sk -o /dev/null -w
      '%{http_code}' -X PROPFIND
      \"https://\$MEDIATION/mediation/disconnect/content\"); [[ \"\$code\" =~
      ^2[0-9]{2}\$ ]] && echo VULNERABLE || { [ \"\$code\" = \"403\" ] && echo
      SAFE || echo \"UNKNOWN (\$code)\"; }"
```

Remplacez `mediation.example.com` par le nom DNS ou l'adresse IP Web de votre serveur Mediation Controller.

Dans une architecture en Cluster, exécutez la commande trois fois : une fois avec la RIP Web de chacun des deux Mediation Controller, puis une fois avec la VIP Web du Cluster.

Cette commande peut être exécutée depuis toute machine Linux disposant d'un accès au serveur Web de **cyber**elements Gate/Cleanroom.

Si le serveur est correctement patché, la commande renvoie `SAFE`. À l'inverse, si le serveur est vulnérable, elle renvoie `VULNERABLE`.

SYSTANCIA

Téléphone : 03 89 33 58 20

Fax : 03 89 33 58 21

site web : https://www.sep.systancia.com