# Impact d'un correctif de sécurité relatif la communication multiposte

## Versions

12.0.31

15.2.12

16.3.1

Siège social
18bis, Allée des Petits Brivins
44500 La Baule-Escoublac

02.40.11.33.60 – contact@atys-concept.com
wwww.atys-concept.com

Agence Sud-Ouest
Central Parc B
56 boulevard de l'Embouchure
31200 Toulouse

SAS au capital de 87 500 € RCS Saint-Nazaire 409 016 599 - APE 4669 B - SIRET 409 016 599 00113 - N°TVA intracommunautaire FR03409016599

# Sommaire


1 Introduction ..... 3
1.1 Impact de la mise à jour ..... 3
1.2 Messages visibles dans l'observateurs d'évènements ..... 4
1.3 Modification de l'option en PcVue 12.0.31 et PcVue 15.2.12 ..... 5
1.3.1 Autorisation pour tous les postes ..... 5
1.3.2 Autorisation pour un poste ..... 5
1.4 Modification de l'option en PcVue 16.3.1 ..... 6
1.4.1 Autorisation pour tous les postes ..... 6
1.4.2 Autorisation pour un poste ..... 6
2 Stratégies de déploiement envisageables ..... 7
2.1 Stratégie 1 : 2 serveurs actifs en simultané ..... 7
2.2 Stratégie 2 - Arrêt simultané des serveurs ..... 8

# 1 Introduction

Des failles de sécurité concernant le multiposte ont été corrigées dans les versions 12.0.31, 15.2.12 et 16.3.1 de PcVue. Il s'agit des vulnérabilités numérotées CVE-2025-9998, CVE-2025-9999.

Retrouvez des informations sur https://www.pcvue.com/security.

Le déploiement des mises à jour de PcVue depuis des versions inférieures à ces versions vers des versions supérieures ou égales à 16.3.1, 15.2.12 et 12.0.31 doit donc être considéré avec la plus grande attention **dans le cas d'architectures multiposte**.

## 1.1 Impact de la mise à jour

Un poste mis à jour avec une version PcVue à partir de 16.3.1, 15.2.12 et 12.0.31 **ne communiquera plus avec les postes de l'architecture en version inférieure** lors de son démarrage. Différents cas peuvent se produire par exemple :

- Dans une association temps réel à serveur actif unique, si un seul des serveurs est mis à jour alors il ne se connectera pas au second serveur, les deux serveurs seront donc actifs simultanément
- Dans une association historique à serveur actif unique (HDS), si un seul des serveurs est mis à jour alors il ne se connectera pas au second serveur, les deux serveurs seront donc actifs simultanément et chercheront à écrire des informations en base de données.
- Si un client est mis à jour il ne pourra pas se connecter à un serveur non mis à jour

Il est bien sûr recommandé de mettre à jour tous les postes afin que l'installation soit protégée contre cette faille. Cependant le temps de la mise à jour les connexions entre postes ne se feront qu'entre postes de même version de PcVue, un plan de déploiement précis doit donc être réfléchi pour assurer la disponibilité du système de supervision.

Dans le cas où la mise à jour de tous les postes n'est pas réalisable rapidement, il est possible d'autoriser la connexion de poste en version précédente sur de postes en nouvelle version afin d'assurer une continuité de service. Cette solution ne doit être que temporaire et une fois tous les postes à jour, **nous vous recommandons de désactiver cette autorisation pour ne plus être exposé à cette faille**.

## 1.2 Messages visibles dans l'observateurs d'évènements

Lorsque qu'un poste en 12.0.31 (ou +) reçoit une tentative de connexion depuis un poste en version antérieure voici le message d'avertissement apparaissant dans l'observateur d'évènements.

2025/09/04,15:20:18.193,3,W,,3722,,101,Mult-postes, Attention, la compatibilité réseau avec la version précédente est rompue. Veuillez ajuster les paramètres d'interopérabilité pour maintenir la compatibilité

Lorsque qu'un poste en 15.2.12 (ou +) reçoit une tentative de connexion depuis un poste en version antérieure voici le message d'avertissement apparaissant dans l'observateur d'évènements.

2025/09/04,14:50:23.445,3,W,,3712,,102, Networking, the version '152010' of the remote station 'SRV1' is not compatible due to security constraints

Lorsque qu'un poste en 16.3.1 (ou +) reçoit une tentative de connexion depuis un poste en version antérieure voici le message d'avertissement apparaissant dans l'observateur d'évènements.

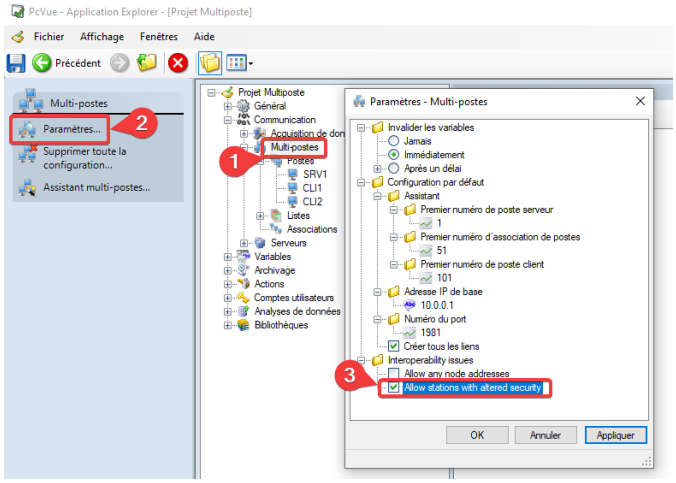
2025/09/04,15:20:18.193,3,W,,3722,,101,Mult-postes, Attention, la compatibilité réseau avec la version précédente est rompue. Veuillez ajuster les paramètres d'interopérabilité pour maintenir la compatibilité.

## 1.3 Modification de l'option en PcVue 12.0.31 et PcVue 15.2.12

Pour autoriser la connexion multipostes avec les anciennes versions (inférieures à 12.0.31 et 15.2.12), ouvrir le projet en nouvelle version 12.0.31 ou 15.2.12 sur un poste de développement.

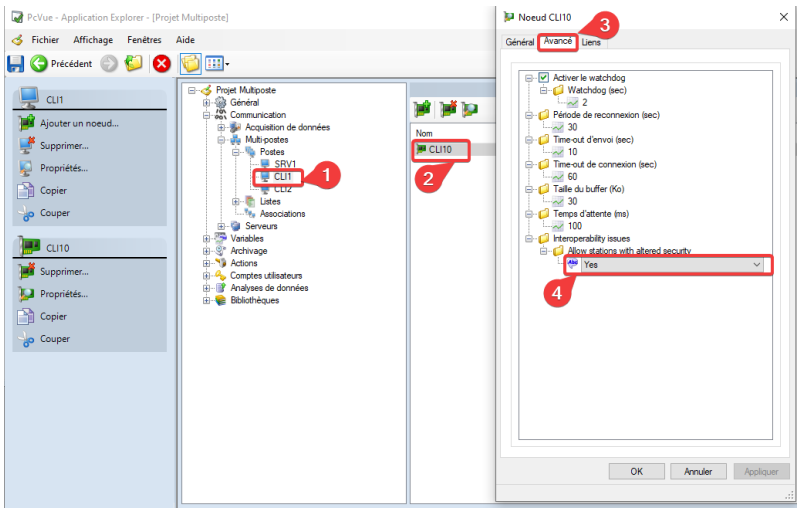
### 1.3.1 Autorisation pour tous les postes

Pour autoriser la connexion avec les anciennes versions pour tous les postes, il faut aller dans les paramètres Multi-postes et activer la propriété **Allow stations with altered security** comme illustré ci-dessous :




### 1.3.2 Autorisation pour un poste

Pour n'autoriser que certains postes à utiliser le mode de sécurité altéré, ouvrir les propriétés du nœud de ce poste et configurer la propriété **Allow stations with altered security** à **Yes**.

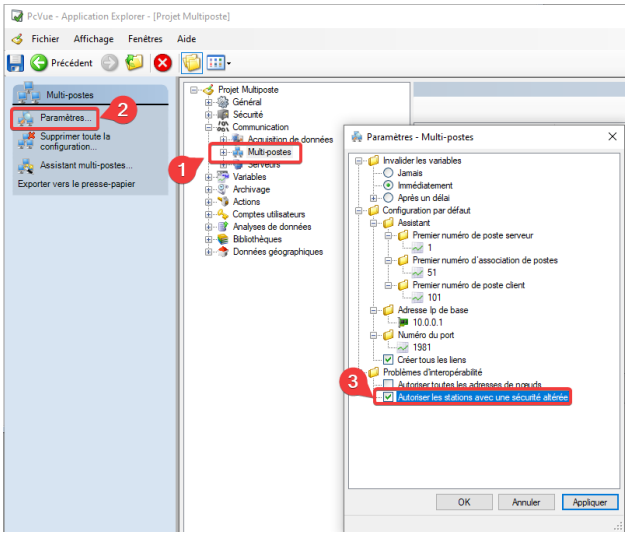


## 1.4 Modification de l'option en PcVue 16.3.1

Pour autoriser la connexion des potes avec les anciennes versions, ouvrir le projet en nouvelle version 16.3.1 (ou +) sur un poste de développement.

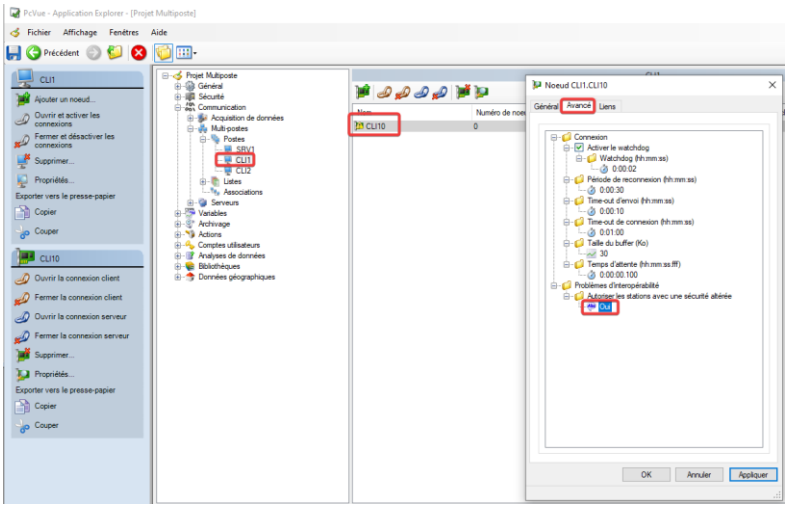
### 1.4.1 Autorisation pour tous les postes

Pour autoriser la connexion avec les anciennes versions pour tous les postes, il faut aller dans les paramètres Multi-postes et activer la propriété **Autoriser les stations avec une sécurité altérée** comme illustré ci-dessous :




### 1.4.2 Autorisation pour un poste

Pour n'autoriser que certains postes à utiliser le mode de sécurité altéré, ouvrir les propriétés du nœud de ce poste et configurer la propriété **Autoriser les stations avec une sécurité** à **Oui**.



# 2 Stratégies de déploiement envisageables

Considérons une architecture multiposte classique composée de :

- 2 serveurs temps réel en association à serveur actif unique
- 2 serveurs (les mêmes que pour le temps réel) en association à serveur actif unique (base de données HDS centralisée)
- 2 clients
- Un poste de développement

Deux stratégies de déploiement sont possibles :

- L'une dans laquelle une version de projet temporaire doit être créée et nécessite le redémarrage à 2 reprises de chacun des postes.
- L'une dans laquelle un seul redémarrage des postes est nécessaire mais dans laquelle les 2 serveurs seront actifs simultanément le temps que ces 2 serveurs soient mis à jour.

## 2.1 Mise à jour en 2 phases

1. Mettre à jour PcVue sur le poste de développement avec la version 16.3.1 (idem 12.0.31 15.2.12).

2. Créer une version de l'application en activant l'option « **Autoriser les stations avec une sécurité altérée »,** la définir comme version de référence.

3. Arrêter tour à tour chacun des postes PcVue, les patcher en version 16.3.1 et redémarrer PcVue.

4. A ce stade tous les postes ont une version de PcVue identique et communiquent entre eux mais autorisent tout de même la connexion de poste avec une sécurité altérée (ils sont sensibles à la faille).

5. Depuis le poste développement créer une nouvelle version en désactivant l'option « **Autoriser les stations avec une sécurité altérée »,** la définir comme version de référence.

6. Mettre à jour l'application sur un premier poste et le redémarrer : celui-ci n'est alors plus sensible à cette faille (et communique toujours avec les autres postes). Redémarrer ainsi PcVue (pour mise à jour de la version d'application) sur l'ensemble des postes.

## 2.2 Mise à jour en 1 phase

Dans cette stratégie on tolère que les deux serveurs soient actifs simultanément un bref instant. L'impact à mesurer ici est la surcharge ponctuelle de la communication vue des équipements (sollicités par les deux serveurs) et des enregistrements historiques potentiellement doublés (sauf cas d'utilisation de protocoles horodatés à la source).

Dans cette stratégie, l'option « Autoriser les stations avec sécurité altérée » n'est pas activée et la mise à jour s'effectue en une seule fois. Cependant, avec cette méthode les postes en version précédente de PcVue ne pourront pas se connecter aux postes mis à jour. Dans le cas d'architecture à serveurs redondants, lorsqu'un seul serveur a été mis à jour alors les 2 serveurs ne se connectent pas et les 2 sont actifs simultanément.

1. Arrêter PcVue sur le poste serveur n°1 et mettre à jour ce poste avec la version 16.3.1 (idem 12.0.31 15.2.12). Redémarrer ce poste serveur n°1. A partir de ce moment les 2 postes serveurs sont actifs.

2. Arrêter tour à tour chacun des postes clients PcVue, les patcher en version 16.3.1 et redémarrer PcVue. Après redémarrage le poste client se connecte au poste serveur n°1 mis à jour précédemment.

3. Une fois tous les postes clients mis à jour, arrêter PcVue sur le poste serveur n°2 et le mettre à jour.

4. L'ensemble des postes est alors mis à jour en nouvelle version et n'est plus sensible à la faille de sécurité.