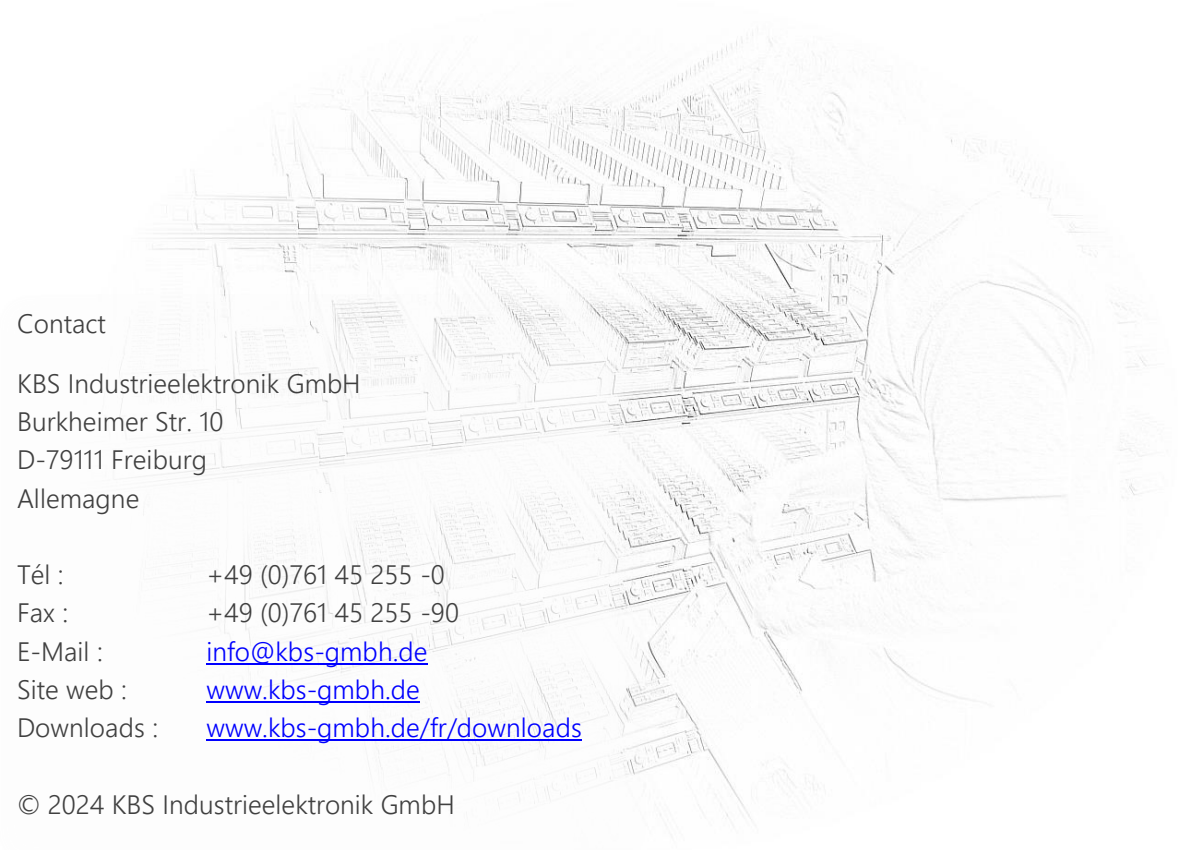
KBS Industrieelektronik GmbH

Avertissement concernant une faille de sécurité dans le logiciel d'interface

PTF Device Manager Windows

(„Winkomm Basis“)

Version : 29|02|2024



Contact

KBS Industrieelektronik GmbH
Burkheimer Str. 10
D-79111 Freiburg
Allemagne

Tél : +49 (0)761 45 255 -0
Fax : +49 (0)761 45 255 -90
E-Mail : info@kbs-gmbh.de
Site web : www.kbs-gmbh.de
Downloads : www.kbs-gmbh.de/fr/downloads

Produit

PTF Device Manager Windows (« Winkomm Basis »)

Description

La faille de sécurité concerne l'accès au logiciel via l'interface web.
Il est possible, en appelant une URL appropriée, de télécharger des fichiers quelconques sur le serveur à partir du lecteur où se trouve le répertoire contenant les fichiers logs.
Dans une installation standard, il s'agit du lecteur C :.

Si l'installation a été effectuée sur un autre lecteur ou si le répertoire des fichiers logs est configuré sur un autre lecteur, c'est l'autre lecteur qui est compromis.

La condition préalable à la composition de l'URL dangereuse est que le nom du fichier et son emplacement soient connus avec précision.

À partir de la version 7.24, cette faille de sécurité est comblée.

Versions concernées

Sont concernées toutes les versions 7 à la version 7.23 pour lesquelles l'interface web est utilisée simultanément.

Mesures possibles

Si l'on parvient à utiliser un lecteur pour stocker les fichiers logs qui ne contient pas d'autres fichiers, aucun dommage ne peut être causé. **Les méthodes suivantes permettent de combler provisoirement la faille de sécurité :**

1. définition d'un nouveau lecteur logique avec les commandes SUBST ou NET USE pour le stockage des fichiers logs

- Pour cela, il faut définir un nouveau lecteur logique. Le nouveau lecteur logique doit correspondre au répertoire dans lequel se trouve le répertoire logfile utilisé.

  Le nouveau lecteur peut être créé à l'aide des commandes Windows SUBST ou NET USE. La commande SUBST est applicable si le répertoire de fichiers logs se trouve sur un lecteur local. La commande NET USE peut être utilisée si les fichiers logs sont placés sur un lecteur réseau.

  P a r t i c u l i è r e m e n t

  Dans une installation standard du logiciel, le répertoire *c:\pdk est* utilisé pour stocker tous les éléments du logiciel. Le répertoire des fichiers logs a alors le chemin *c:\pdk\logfiles*.

Comme le répertoire lofeil se trouve dans le répertoire *c:\PDK,*
le nouveau lecteur doit être créé dans ce cas pour le chemin *C:\PDK*.
Dans cet exemple, la lettre de lecteur choisie est *R* :.

La commande à exécuter dans une fenêtre de ligne de commande ou via un fichier batch est la suivante doit être exécutée est la suivante

SUBST R : C:\PDK

- Dans la configuration de PTF Device Manager, il faut maintenant indiquer le répertoire des fichiers logs sur le nouveau lecteur. Dans ce cas, le chemin est '*R:\Logfiles*'.

La nouvelle lettre de lecteur devient le répertoire racine et ne peut pas être dépassée par les noms de fichiers relatifs, qui sont nécessaires pour l'exploitation de la faille de sécurité.
L'accès à n'importe quel fichier est ainsi bloqué.

2. Définition d'un nom de partage pour le lecteur

- Le répertoire d'installation, qui contient le répertoire avec les fichiers logs, est validé pour utilisation avec le nom de partage. Cette méthode n'est applicable que si le répertoire des fichiers logs se trouve sur un lecteur local. Pour les lecteurs externes, la commande Net USE peut être utilisée (voir ci-dessus).

  Ce partage est créé à l'aide de l'Explorateur Windows.

  Exemple

  Dans une installation standard du logiciel, le répertoire *c:\pdk* est utilisé
  pour stocker toutes les parties du logiciel.

  Le répertoire des fichiers logs a pour chemin d'accès *c:\pdk\logfiles*.
  Avec la fonction 'Autoriser l'accès' de l'Explorateur Windows un partage avec un nom de partage est créé.

- Dans la configuration du PTF Device Manager, il faut maintenant indiquer le nom de l'ordinateur et le nom de partage comme répertoire des fichiers logs. Dans ce cas, le chemin est '\\<nom de l'ordinateur>\<nom du partage>\Logfiles'.

Le partage devient le répertoire racine et ne peut pas être dépassé par les noms de fichiers relatifs nécessaires à l'exploitation de la faille de sécurité. L'accès à n'importe quel fichier est donc bloqué.
Il reste toutefois possible de charger des fichiers depuis le répertoire d'installation du PTF Device Manager.

Pour résoudre le problème sans cette mesure, il faut effectuer une mise à jour ou une mise à niveau vers une version 7.24 ou plus récente.