

**Warnung vor einer Sicherheitslücke
in der Schnittstellen-Software
PTF Device Manager Windows
(Winkomm Basis)**

Stand: 29|02|2024

Kontakt

KBS Industrieelektronik GmbH
Burkheimer Str. 10
D-79111 Freiburg im Breisgau
Germany

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

© 2024 KBS Industrieelektronik GmbH

Produkt

PTF Device Manager Windows (Winkomm Basis)

Beschreibung

Die Sicherheitslücke betrifft den Zugriff auf die Software über das Web-Interface.

Es ist möglich, durch den Abruf einer geeigneten URL beliebige Dateien von dem Laufwerk auf den Server herunterzuladen, auf dem sich das Verzeichnis mit den Logdateien befindet.

In einer Standardinstallation ist das das Laufwerk C:.

Wenn die Installation auf ein anderes Laufwerk vorgenommen wurde oder wenn das Verzeichnis für Logdateien auf einem anderen Laufwerk konfiguriert ist, so ist das andere das gefährdete Laufwerk.

Voraussetzung für die Zusammenstellung der gefährlichen URL ist, dass der Name der Datei und der Speicherort genau bekannt sind.

Ab der Version 7.24 ist diese Sicherheitslücke geschlossen.

Betroffene Versionen

Betroffen sind alle Versionen 7 bis zur Version 7.23, bei denen gleichzeitig das Webinterface genutzt wird.

Mögliche Maßnahmen

Wenn es gelingt, ein Laufwerk zur Speicherung der Logdateien zu nutzen, das keine anderen Dateien enthält, kann kein Schaden entstehen. **Mit folgenden Methoden kann die Sicherheitslücke provisorisch geschlossen werden:**

1. Definition eines neuen logischen Laufwerks mit den Befehlen SUBST oder NET USE für die Speicherung der Logdateien

- Dazu muss ein neues logisches Laufwerk definiert werden. Das neue logische Laufwerk muss auf das Verzeichnis abbilden, in welchem das verwendete Logfile-Verzeichnis liegt.

Das neue Laufwerk kann mit den Windows-Befehlen SUBST bzw. mit NET USE angelegt werden. Der Befehl SUBST ist anwendbar, wenn das Logfile-Verzeichnis auf einem lokalen Laufwerk liegt. Der Befehl NET USE kann genutzt werden, wenn die Logfiles auf einem Netzwerk-Laufwerk abgelegt werden.

Beispiel

In einer Standardinstallation der Software wird das Verzeichnis `c:\pdk` benutzt, um alle Teile der Software abzulegen. Das Logdatei-Verzeichnis hat dann den Pfad

c:\pdk\logfiles. Da sich das Logfile-Verzeichnis im Verzeichnis c:\PDK befinden, muss das neue Laufwerk in diesem Fall für den Pfad C:\PDK angelegt werden. In diesem Beispiel wurde als Laufwerksbuchstabe R: gewählt.

Der Befehl, der in einem Kommandozeilenfenster oder über eine Batch-datei ausgeführt werden muss, lautet:

```
SUBST R: C:\PDK
```

- In der Konfiguration des PTF Device Manager muss nun als Logdatei-Verzeichnis auf dem neuen Laufwerk angegeben werden. Der Pfad lautet in diesem Fall 'R:\Logfiles'

Der neue Laufwerksbuchstabe wird zum Wurzelverzeichnis und kann von relativen Dateinamen, die für die Ausnutzung der Sicherheitslücke notwendig sind, nicht überschritten werden. Es wird damit der Zugriff auf beliebige Dateien blockiert.

2. Definition eines Freigabens für das Laufwerk

- Das Installationsverzeichnis, welches das Logfileverzeichnis enthält, wird für die Nutzung unter dem Freigabennamen freigegeben. Diese Methode ist nur anwendbar, wenn das Logfile-Verzeichnis auf einem lokalen Laufwerk liegt. Für externe Laufwerke kann der Befehl Net USE verwendet werden (siehe oben)

Diese Freigabe wird mit dem Windows Explorer angelegt.

Beispiel

In einer Standardinstallation der Software wird das Verzeichnis c:\pdk benutzt, um alle Teile der Software abzulegen.

Das Logdatei-Verzeichnis hat den Pfad c:\pdk\logfiles.

Mit der Funktion 'Zugriff Gewähren' im Windows Explorer wird eine Freigabe mit einem Freigabennamen erstellt.

- In der Konfiguration des PTF Device Manager muss nun als Logdatei-Verzeichnis der Rechnername und der Freigabename angegeben werden. Der Pfad lautet in diesem Fall '\\<Rechnername>\<Freigabename>\Logfiles'

Die Freigabe wird zum Wurzelverzeichnis und kann von relativen Dateinamen, die für die Ausnutzung der Sicherheitslücke notwendig sind, nicht überschritten werden. Es wird damit der Zugriff auf beliebige Dateien blockiert.

Die Möglichkeit, Dateien aus dem Installationsverzeichnis des PTF Device Managers zu laden, besteht jedoch weiterhin.

Um das Problem ohne diese Maßnahme zu lösen, muss ein Update oder Upgrade auf eine Version 7.24 oder neuer durchgeführt werden.