KBS Industrieelektronik GmbH

Warning of security vulnerability

in interface software

PTF Device Manager Windows

(Winkomm Basis)

Status: February 29, 2024

Contact

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

Phone: +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/en/downloads

Product

PTF Device Manager Windows (Winkomm Basis)

Description

The security vulnerability affects access to the software via the web interface. It is possible to download any file from the drive on the server where the directory with the log files is located by calling up a suitable URL. In a standard installation, this is the C: drive.

If the installation was carried out on a different drive or if the directory for log files is configured on a different drive, the other drive is the vulnerable drive.

The prerequisite for compiling the dangerous URL is that the name of the file and the storage location are known exactly.

This vulnerability has been closed in versions 7.24 and higher.

Affected versions

All versions 7 up to version 7.23 are affected if the web interface is used at the same time.

Possible measures

If it is possible to use a drive to store the log files that does not contain any other files, no damage can occur. **The following methods can be used to provisionally close the security gap:**

1. **Definition of a new logical drive with the SUBST or NET USE commands for storing the log files**

   - A new logical drive must be defined for this purpose. The new logical drive must map to the directory in which the log file directory used is located.

     The new drive can be created with the Windows commands SUBST or NET USE.
     The SUBST command can be used if the log file directory is located on a local drive.
     The NET USE command can be used if the log files are stored on a network drive.

     EXAMPLE:

     In a standard installation of the software, the directory *c:\pdk* is used to store all parts of the software. The log file directory then has the path *c:\pdk\logfiles*. As the log files directory is located under the directory *c:\PDK*, the new drive must be created for the path *C:\PDK* in this case. In this example, R: was selected as the drive letter.

     The command that must be executed in a command line window or via a batch file is

     SUBST R: C:\PDK

- The log file directory on the new drive must now be specified in the configuration of the PTF Device Manager. In this case, the path is '*R:\Logfiles*'

The new drive letter becomes the root directory and cannot be exceeded by relative file names, which are necessary for exploiting the vulnerability. This blocks access to other files.

2. Definition of a share name for the drive

- The installation directory containing the log file directory is released for use under the share name. This method can only be used if the log file directory is located on a local drive. The Net USE command can be used for external drives (see above).

  This share is created with Windows Explorer.

  EXAMPLE:

  In a standard installation of the software, the directory *c:\pdk* is used to store all parts of the software.

  The log file directory has the path c:\pdk\logfiles. A share with a share name is created using the 'Grant access' function in Windows Explorer.

- In the configuration of the PTF Device Manager, the computer name and the share name must now be specified as the log file directory. In this case, the path is '\\<computer name>\<share name>\Logfiles'.

The share becomes the root directory and cannot be exceeded by relative file names, which are necessary for exploiting the vulnerability. This blocks access to any files.

However, it is still possible to load files from the installation directory of the PTF Device Manager, i.e. files belonging to the PTF Device Manager.

To solve the problem without this measure, an update or upgrade to version 7.24 or later must be carried out.