Windows Privilege Escalation

Security Advisory for CVE-2020-26155

Creating Trust in the Digital Society

utimaco®

1 Issue

1.1 Description

UTIMACO has been made aware of a vulnerability affecting the Windows installations of product packages regarding the following affected UTIMACO Product(s), component(s) and version(s):

- SecurityServer 3.x, 4.x up to version 4.31.1
- PaymentServer 3.x, 4.x up to version 4.33.0
- PaymentServer Hybrid 3.x, 4.x up to version 4.33.0
- Block-safe 2.0.0, 3.0.0
- CryptoServer CP5 5.0.0.0, 5.1.0.0, incl. CryptoServer CP5 Supporting CD and CryptoServer CP5 SDK CD
- CryptoServer CP5 VS-NfD 5.1.0.0
- CryptoServer SDK 3.x, 4.x up to version 4.31.1

hereinafter collectively referred to as “Affected Products”.

When installing product packages of the Affected Products, using the Windows installer shipped on the product CD, incorrect folder permissions are configured. Also, the PIN Pad Daemon “PPD” is configured to run under LocalSystem account. Both could allow for an attacker to escalate Windows privileges from a standard “Authenticated User” to that of an Administrator or SYSTEM.

1.2 Issue ID

This issue has been reserved in the Common Vulnerabilities and Exposures list as CVE-2020-26155.
Details will be published end of January 2021 on the CVE website https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26155.

Do not disclose this vulnerability before its publication on the CVE website to give all affected customers due time for fixing their installations.

1.3 Detailed description

The Windows installer shipped with UTIMACO product CD’s for the Affected Products grants full permissions for “Authenticated Users” to the product installation folder. Therefore, it would be possible for a user whose credential is validated by Windows OS to replace or modify program binaries with malicious files, which could then be leveraged for diverse attack scenarios including Windows privilege escalations.

Additionally, the installer adds some of the installation sub-folders to the PATH variable. This can be used by the same users to perform DLL hijacking/sideloading attacks.

Finally, the PIN Pad Daemon “PPD” service is registered without quoting the binary path name and to run under LocalSystem account. Depending on the path name or in conjunction with the writable installation sub-folders this can as well be abused to load malicious binaries and execute with SYSTEM privileges.

Please note that HSM firmware is not affected by this vulnerability.

2 What To Do

Please follow the instructions below if you have installed an Affected Product. The instructions differ depending on the affected product and maintenance status:

- For SecurityServer 4.31.0 and SecurityServer 4.31.1, you should update your installation to SecurityServer 4.31.2 as described in section 2.1 if you have a maintenance contract.
- For SecurityServer installations older than SecurityServer 4.31.0, we strongly recommend you upgrade your installation to SecurityServer 4.31.2 if you have a valid maintenance contract. If you do not have a maintenance contract or if you do not want to upgrade you may alternatively apply a hotfix to the currently installed version. Please follow the guidance in section 2.2.
- For other affected products or customers without a maintenance contract you should run the hotfix as described in section 2.3.

SecurityServer 4.31.2 and the hotfix are available in the Downloads section of the UTIMACO support portal https://support.hsm.utimaco.com/support/downloads. Login to the support portal is required.

For customers with maintenance contract: a new release is available in your product download section and in the SecurityServer HotFixes and Patches section.

For all others: the patch is available in the hotfixes and patches section.

2.1 Updating SecurityServer 4.31.0 and SecurityServer 4.31.1

UTIMACO has released SecurityServer 4.31.2 that fixes the access permissions set by the installer and the PPD registration. Proceed as follows after login to the support portal:

- On the Downloads page, scroll down to the SecurityServer section that matches your HSM platform, e.g. “SecurityServer Se Gen2”, then select “Show Downloads”.
- Select “4.31.2” in the “Versions” section of the Downloads page and download the file SecurityServer-V4.31.2.0.zip to your computer. Unzip this file to some temporary directory, e.g. C:\temp.
- Before installing the new version, make sure that you uninstall your current installation. Right click on the Windows Start button, then select ‘Apps & Features’. Start typing “CryptoServer” in the search field of the Apps & Features window, and Windows will find the CryptoServer app. Click on the CryptoServer app and press the ‘Uninstall’ button to uninstall the current installation. Alternatively, you may open the Control Panel, and select ‘Uninstall a program’ from the ‘Programs’ section, and Windows will find the CryptoServer program. Either double-click on the CryptoServer program or press the ‘Uninstall’ button to uninstall the current installation. Configuration files will not be removed from directory C:\ProgramData\Utimaco during uninstallation.
- To be sure that a possible exploitation of the vulnerability gets fixed, it is important that the previous installation is removed completely. You should therefore open Windows File Explorer, a command shell or PowerShell and check that the previous installation has been removed completely, i.e. there is no more directory “Utimaco” in “C:\Program Files”. In case the “Utimaco” directory has not been removed, delete it manually.
- Now install SecurityServer 4.31.2 from the location where you have saved the unzipped product CD, e.g. C:\temp, by executing CryptoServerSetup-4.31.2.0.exe. Instruct the installer to not overwrite existing configuration files when being asked; your previous configuration files in directory C:\ProgramData\Utimaco will then be taken over.
- In case your previous installed version was SecurityServer 4.31.0, make sure you update your HSM firmware to profit from bug fixes introduced since then.

2.2 Upgrading or fixing SecurityServer installations older than 4.31.0

If you have installed a SecurityServer version older than SecurityServer 4.31.0, we strongly recommend you upgrade to SecurityServer 4.31.2. If you have a valid maintenance contract please consult the release notes of SecurityServer versions which are more recent than your installation and make yourself familiar with all new, legacy and discontinued features. You find these release notes on the Downloads page of the support portal:

- Scroll down to the SecurityServer section that matches your HSM platform, e.g. “SecurityServer Se Gen2”, then select “Show Downloads”.

- In the “Versions” section of the Downloads page, select the version(s) that are more recent than your current installation, and consult the release notes in the “Getting Started” section.

In case you choose to upgrade your installation to SecurityServer 4.31.2 you should proceed as described in section 2.1 above. Make sure that you also upgrade the HSM firmware to ensure full functionality of your installation.

If you decide to not upgrade to SecurityServer 4.31.2, you should apply the hotfix as described in the following section 2.3.

2.3 Applying the hotfix

Please follow the instructions below if you have installed an Affected Product other than SecurityServer or if you cannot upgrade your SecurityServer installation to version 4.31.2.

UTIMACO has released a patch in form of an executable batch file that fixes the access permissions and PPD registration. This patch is available in our support portal under https://support.hsm.utimaco.com/securityserver-hotfixes-and-patches. Customers with a maintenance contract will also find it in the product download section. Login to the support portal is required. Download the patch and save the file on your computer.

The patch cannot detect whether the vulnerability has already been exploited in your installation. We therefore strongly recommend that you uninstall and completely remove your current installation.

- Right click on the Windows Start button, then select ‘Apps & Features’ and search for the product that is currently installed, e.g. PaymentServer. Select that app and press the ‘Uninstall’ button to uninstall the current installation. Alternatively, you may open the Control Panel, select ‘Uninstall a program‘ from the ‘Programs’ section; in the list of programs, select the product that is currently installed, e.g. PaymentServer, and either double-click on that program or press the ‘Uninstall’ button to uninstall the current installation. Configuration files will not be removed from directory C:\ProgramData\Utimaco during uninstallation.

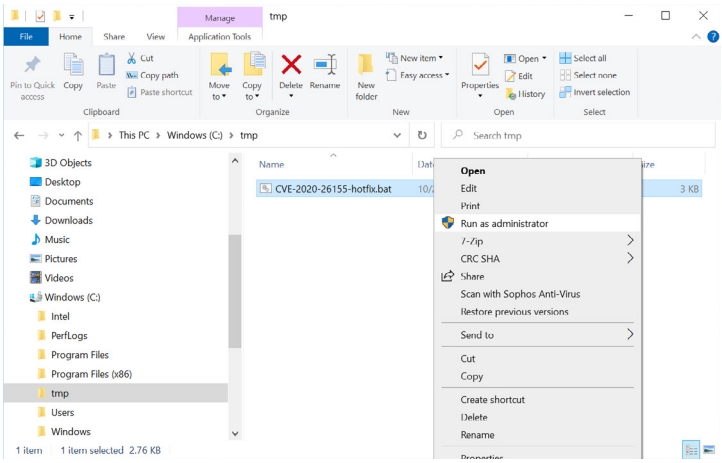
- It is important that the previous installation is removed completely. You should therefore open Windows File Explorer, a command shell or PowerShell and check that the previous installation has been removed completely, i.e. there is no more directory “Utimaco” in “C:\Program Files”. In case the “Utimaco” directory has not been removed, delete it manually.

- Install your product package again which was shipped to you together with the appliance or PCIe card. Instruct the installer to not overwrite existing configuration files when being asked; your previous configuration files in directory C:\ProgramData\Utimaco will then be taken over.

Now apply the hotfix as follows:

For SecurityServer, CryptoServer SDK and CryptoServer CP5 run it with Administrator privileges. To do so, right-click on the file and select “Run as administrator” from the context menu.

The fix will run automatically and show a message if successful or an error otherwise. In case the fix has successfully applied correct permissions, you may close the command shell.



If the window closes immediately an unexpected error has occurred. Please run the hotfix from a command line as described in the following section, but without specifying a parameter.

For PaymentServer, PaymentServer Hybrid and Block-safe open an Administrator command shell first. To do so, click on the Windows start symbol, type “command”, right-click on “Command Prompt” and select “Run as administrator”. On Windows 10, you’ll find it also in the menu under “Windows System”. Type “CVE-2020-26155-hotfix „<path>“” and replace <path> with the full name of the installation folder. For PaymentServer, this is typically “C:\Program Files\Utimaco\PaymentServer”. Therefore, the full command for PaymentServer would be:

```
CVE-2020-26155-hotfix "C:\Program Files\Utimaco\PaymentServer"
```

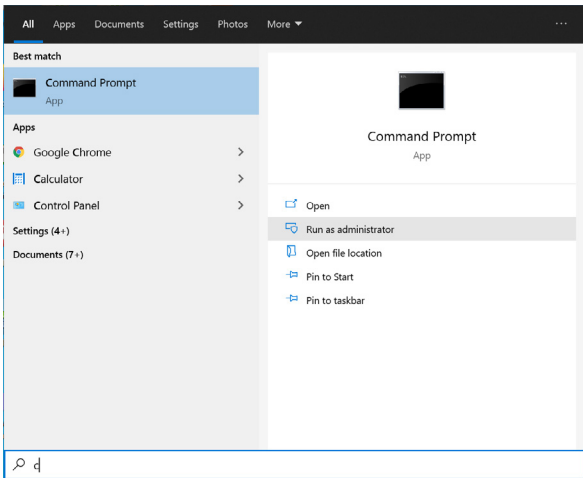
The fix will run automatically and show a message if successful or an error otherwise.

2.4 Manual Procedures

If you have a non-standard installation or if the hotfix described under section 2.3 fails, you might need to apply the changes manually. In doubt contact your administrator or UTIMACO’s Technical Support (contact details under section 5).

Open a command shell with administrator privileges.

To do so, click on the Windows start symbol, type “command”, right-click on “Command Prompt” and select “Run as administrator”. (On Windows 10, you’ll find it also in the menu under “Windows System”.)



Perform the following actions to fix the permission settings for all affected products except CryptoServer SDK, for which see below

- Change to the root installation directory of the affected product. In case of installation into the default directory, the command is

```
cd "\Program Files\Utimaco\CryptoServer"
```

- Reset the permission using

  icacls . /reset /t

- If the software is installed outside of “Program Files” disable permission inheritance and remove privileges for “Authenticated Users” using:

  icacls . /inheritance:d

  icacls . /remove "Authenticated Users"

- If you have the simulator installed, grant “modify” permissions to its working directory.

  For SecurityServer, PaymentServer, CryptoServer CP5 and CryptoServer CP5 NfD:

  icacls Simulator\sim5_windows\devices /grant "Authenticated Users":(OI)(CI)M

- For PaymentServer Hybrid:

  icacls Simulator\sim5_cxi_windows\devices /grant "Authenticated Users":(OI)(CI)M

- For Block-safe:

  icacls Simulator\sim5_bs_windows\devices /grant "Authenticated Users":(OI)(CI)M

Perform the following actions to fix the permission settings for CryptoServer SDK:

- Change to the root installation directory of the CryptoServer SDK. In case of installation into the default directory, the command is

  cd \Utimaco\CryptoServer

- Reset the permission using

  icacls . /reset /t

- Disable permission inheritance and remove privileges for “Authenticated Users” using:

  icacls . /inheritance:d

  icacls . /remove "Authenticated Users"

- If you have the simulator installed, grant “modify” permissions to its working directory.

  icacls SDK\devices /grant "Authenticated Users":(OI)(CI)M

If the PIN Pad Daemon “PPD” is installed, perform the following actions to change its registration.

- Run the following command in your command shell:

  sc qc ppd

If this command returns with an error, then PPD is not installed und you may skip the following steps.

```
C:\Program Files\Utimaco\CryptoServer\Administration>sc qc PPD
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: PPD
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : "C:\Program Files\Utimaco\CryptoServer\Administration\ppd.exe"
        LOAD_ORDER_GROUP   : Extended Base
        TAG                : 0
        DISPLAY_NAME       : PIN Pad Daemon
        DEPENDENCIES       :
        SERVICE_START_NAME : NT AUTHORITY\LocalService

C:\Program Files\Utimaco\CryptoServer\Administration>_
```

- Look for the “BINARY_PATH_NAME :” line in the output, copy the part after the “:” (hereinafter referred to as “BINPATH”) and paste it into some text editor, e.g. Notepad.
- BINPATH consists of the actual path to ppd.exe and an optional “-config=…” part. Both parts need to be treated separately.
  - Insert “\”” before and after the first part, i.e. the path to ppd.exe.
  - In the optional second part, replace each “”” (double quote) with “\””.

Examples:

Without optional “-config=…” part, change

C:\Program Files\Utimaco\CryptoServer\Administration\ppd.exe

to

\"C:\Program Files\Utimaco\CryptoServer\Administration\ppd.exe\"

With optional “-config=…” part, change

C:\Program Files\Utimaco\CryptoServer\Administration\ppd.exe

-config="C:\ProgramData\Utimaco\PPD\ppd.cfg"

to

\"C:\Program Files\Utimaco\CryptoServer\Administration\ppd.exe\"

-config=\"C:\ProgramData\Utimaco\PPD\ppd.cfg\"

Run the following command, where you replace BINPATH with the text you have edited in your text editor:

sc config PPD binPath="BINPATH" obj="NT AUTHORITY\LocalService"

```
C:\Program Files\Utimaco\CryptoServer\Administration>sc config PPD binpath="\"C:\Program Files\Utimaco\CryptoServer\Admi
nistration\ppd.exe\"" obj="NT AUTHORITY\LocalService"
[SC] ChangeServiceConfig SUCCESS

C:\Program Files\Utimaco\CryptoServer\Administration>
```

If you need more information or guidance, please contact our Technical Support (contact details in section 5).

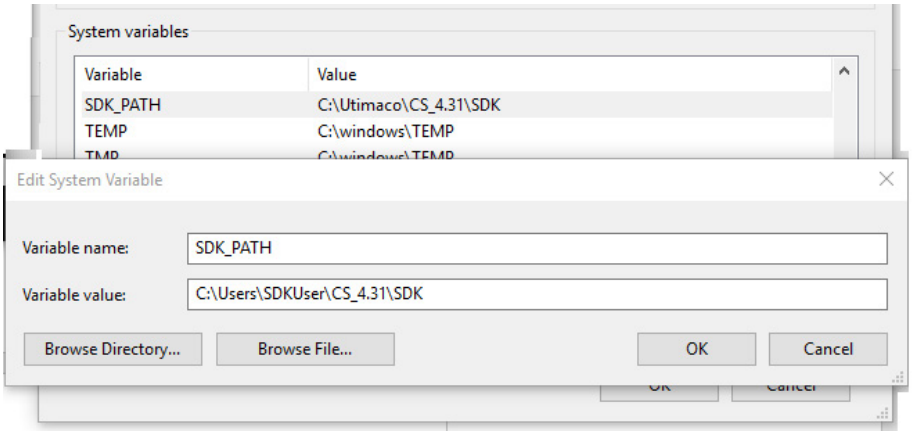
3 Side Effects

After applying the patch in accordance with section 2, you will not be able to change or compile the example files shipped with the software, where they are installed. Therefore copy them to your usual development working directory first.

For debugging an SDK module, the module DLL needs to be copied into the Simulator's bin folder (usually "C:\Utimaco\CryptoServer\SDK\bin"). After applying the patch this folder is write protected. Copy the complete SDK folder to your usual development working directory, and set the SDK_PATH environment variable to point to it. In the Windows Start menu, type 'edit the system' and select the offered "Edit the system environment variables".

In the dialog, click on 'Environment Variables…'.

In the Environment Variables dialog, for User or System, create or edit the SDK_PATH variable, and set it to point at the location of your copied SDK development tree.



The Debugger will now pick up the Simulator at %SDK_PATH%\bin\bl_sim5.exe, and the compiler rule that copies the generated debug .DLL into the Simulator's working directory will also correctly point to the new location.

Alternately, in the Visual Studio properties of the project, you can change the "Command" in "Debugging" to point to "bl_sim5.exe" in the new Simulator bin folder and change either the "Output File" in "Linker – General" or the "Command Line" in "Build Events – Post-Build Event" to store the resulting DLL to the same directory.

4 Fix in next releases

UTIMACO will include the changes of the hotfix in the next product releases:

- SecurityServer 4.31.2, available now
- PaymentServer 4.34
- PaymentServer Hybrid 4.34
- Block-safe 4.34
- CryptoServer CP5 5.1.0.1
- CryptoServer CP5 VS-NfD 5.1.0.1
- CryptoServer SDK 4.40, targeted for mid January 2021

Products without target date in the overview above are currently in planning. Reach out to your UTIMACO Sales or Support contact for an update.

5 Technical support

You can find technical support for UTIMACO products in any of these ways:

Download product information from https://hsm.utimaco.com/cryptoserver/ .

Contact us at https://hsm.utimaco.com/company/contact/.

Send an email to support-cs@utimaco.com, including your hardware serial number(s), software version number(s), operating system(s) and patch level(s), and the text of any error messages.

Contact our support hotline: **EMEA** +49 800-627-3081, **Americas** +1-844-UTIMACO (+1 844-884-6226), **APAC** +81 800-919-1301.

6 Legal notices

This “SecurityServer Advisory Windows Permissions” is subject to the effective agreement executed between you and Utimaco IS GmbH, Utimaco Inc. or Utimaco IS Pte Ltd. or otherwise the General Terms and Conditions of Utimaco: https://hsm.utimaco.com/terms-and-conditions/

Get in Touch

EMEA

UTIMACO IS GmbH

Germanusstrasse 4
52080 Aachen,
Germany

+49 241 1696 200

hsm@utimaco.com

Americas

UTIMACO Inc.

900 E Hamilton Ave., Suite 400
Campbell, CA 95008,
USA

+1 844 UTIMACO

hsm@utimaco.com

APAC

UTIMACO IS Pte Limited

50 Raffles Place,
Level 19, Singapore Land Tower,
Singapore 048623

+65 6631 2758

hsm@utimaco.com

For more information about UTIMACO® HSM products, please visit:
hsm.utimaco.com

Creating Trust in
the **Digital Society**

utimaco®