PRODUCT SECURITY ADVISORY

CSRF in OMNIKEY 5x27 Desktop Readers

TLP:WHITE

No restriction on distribution.

HID-PSA-2020-001
02-November-2020

Severity: CRITICAL

CVSS 9.6 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H)

Overview:

The OMNIKEY® 5427 and OMNIKEY 5127 readers allow loading configurations to the reader using the EEM driver (Ethernet Emulation Mode) for the integrated webserver. The configuration file upload request does not check the origin of the request, which would allow a malicious site to upload a configuration file to the device.

Affected Products:

Customers using the EEM driver with OMNIKEY 5427 and OMNIKEY 5127 with the following part numbers:

R54270001-xxx OMNIKEY 5427 Gen 1
R54270101-xxx OMNIKEY 5427 Gen 2
R54270111-xxx OMNIKEY 5427 Gen 2 with BLE interface
R51270010-xxx OMNIKEY 5127 Mini
R51270020-xxx OMNIKEY 5127 Mini with industrial housing
R51270030-xxx OMNIKEY 5127 Reader Core

In order to identify your reader, please review the product label located on the device.

Impact:

If exploited, the malicious site could upload a configuration file to the device. This file may include commands that would be sent to the connected workstation.

Mitigation:

HID Global has created a Service Pack for the OMNIKEY 5427 Gen 2 desktop reader and OMNIKEY 5127 devices to address this issue.

This Electronic Release is available on HID Global's Developer Center portal.

The OMNIKEY 5427 Gen 1 desktop readers are end of life and no Service Pack will be available.

Users may mitigate this issue by disabling the EEM interface using one of the following options:

a. Disable the EEM interface of the reader (using web management interface) as a preferred option. See the OMNIKEY 5x27CK Keyboard Wedge Configuration and Customer Report User Guide, Chapter 6.1
b. Disable using a Config card. See the OMNIKEY 5x27CK Keyboard Wedge Configuration and Customer Report User Guide, Chapter 2.2.4
c. Disable via EEM driver uninstallation / disabling as a backup option. See the OMNIKEY 5x27CK Keyboard Wedge Configuration and Customer Report User Guide, Chapter 2.1.1

To verify if the EEM interface of the reader has been disabled, follow these steps:

1) Connect the reader to a Windows PC. See the OMNIKEY 5x27CK Keyboard Wedge Configuration and Customer Report User Guide, Chapter 2.1.1
2) Start a supported web browser and enter http://192.168.63.99/ in the address bar. See the OMNIKEY 5x27CK Keyboard Wedge Configuration and Customer Report User Guide, Chapter 2.2
    a. If the “OMNIKEY 5427 CK Reader Management” screen is displayed, the EEM interface is enabled
    b. If you receive a “connection timeout” message or something similar, the EEM driver is disabled

To validate if the EEM driver is installed on a Windows PC, go to the Windows Device Manager and connect an OMNIKEY 5427CK reader to the PC. If the driver is available, there will be an entry “HID USBCDC EEM Ethernet Adapter…”) in the “Network adapters” settings.

Contact Information:

For more information, contact your local HID sales representative or HID Global Technical Support Services.

Credit:

HID Global would like to thank Amanda Brown, Alicen DiPiano and Meaghan Longenberger at IBM X-Force Red for responsibly making this disclosure.