July 8, 2021

In June 2020, ID TECH acknowledged an IOActive Advisory written by Josep Pi Rodriguez, which reported a detailed attack performed on a non-PCI PTS Kiosk III device held by Mr. Pi Rodriguez. Throughout the process IOActive has worked closely with ID TECH to responsibly disclose and address the vulnerability.

ID TECH took immediate actions to communicate with IOActive and proceeded to work on solution(s) to address the identified issue.

With prior detailed knowledge of the firmware, IOActive shared how a customized stack overflow attack was used to overflow the stack to control subsequent firmware execution. With control of the firmware execution, an attacker could modify the firmware code in the reader. Use of unauthorized firmware could potentially lead to further attacks on the host system connected to the reader.

The stack overflow exploitation with a non-customized payload leads to the device becoming unresponsive. A power cycle would be required to recover the Kiosk III functionality.

The attack method was investigated across all of ID TECH's products and every product found to be susceptible to an APDU stack overflow attack received a new firmware update. Updated firmware for the Kiosk III was provided to IOActive in October 2020 for testing. IOActive validated and approved the firmware in December 2020 and provided ID TECH a finalized Remediation Report in January 2021. Firmware packages that include the solution on the different products are listed here:

    Kiosk II - GR2.0.0_C57
    Kiosk III - V1.20.132
    Kiosk III - V1.10.173
    Kiosk IV – V1.20.132
    VP3300 BT - V1.01.185 and V1.10.010
    VP3300 USB - V1.01.209 and V1.10.010
    Vendi – V1.00.145.X

ID TECH strongly recommends customers with these products should update to these firmware versions or higher at their earliest convenience. For additional details, please refer to the IOActive advisory available here: https://ioac.tv/36qMUVf

NOTE: *ID TECH does not have any knowledge or evidence of any jackpot attacks actually occurring on ATMs integrated with ID TECH products.*

ID TECH