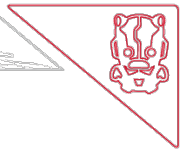
IOActive.
1426 Elliott Avenue W, Seattle, WA 98119
(866) 760.0222 | info@ioactive.com



08 July 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 exploitation was used 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. IOActive successfully developed a jackpot or cash-out proof of concept (POC) on a non-ID TECH hardware device materially similar to the devices covered by the ID TECH advisory.

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.

IOActive strongly recommends that ID TECH customers with affected products should update firmware as soon as practical. For additional details, please refer to the ID TECH advisory available here:

https://idtechproducts.com/id-tech-ioactive-joint-advisory/

IOActive will not be releasing additional technical details publicly at this time. IOActive is coordinating a technical and risk briefing to FS-ISAC members to be released in the near future. The IOActive Responsible Disclosure Policy can be found here: https://ioactive.com/disclosure-policy/