EDITORS' PICK

‘Millions’ Of Payment Terminals Are Vulnerable To Credit Card Theft Hacks

Thomas Brewster Forbes Staff
Senior writer at Forbes covering cybercrime, privacy and surveillance.

Follow

Dec 10, 2020, 06:16am EST

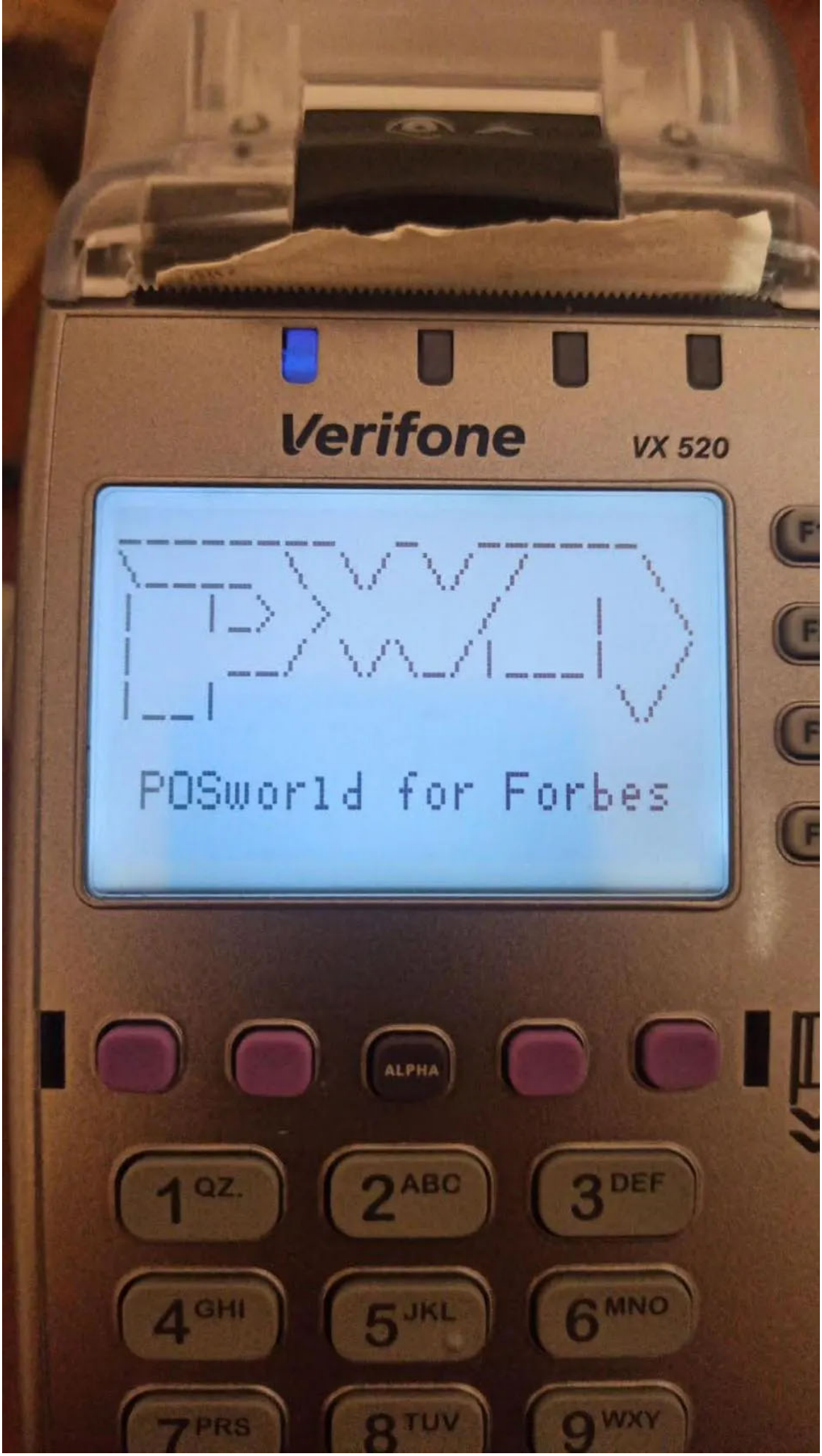
Vulnerable Verifone payment terminals can be hacked if not patched, researchers warn. JEFF GREENBERG/UNIVERSAL IMAGES GROUP VIA GETTY IMAGES

Point-of-sale payment devices made by two of the industry’s biggest manufacturers contained vulnerabilities that made stealing credit card data much simpler. Millions of devices may be affected, according to cybersecurity researchers Timur Yunosov and Aleksei Stennikov, who will present their findings at the Black Hat EU security conference on Thursday.

The weaknesses lay in devices made by Verifone and Ingenico. The first issue was that they used default passwords that let anyone with physical access through to a "service menu." These menus contained functions that could be abused to write malware onto the terminals. The malware could then hoover up credit card numbers once the device was in use again. Though the terminals did encrypt credit card data, they did so on the same internal system already controlled by the malware, rendering it useless. An attacker would have all the information they required to clone cards and start stealing people's money.

The obvious barrier to a successful attack is in being able to get access to a terminal for long enough to download the malware. Yunosov, from the Cyber R&D Lab, said it would take between five and ten minutes to connect to the devices via USB and install the malicious card sniffer. One of the vulnerabilities could also have been exploited over the internal network, so if a hacker found a way onto a shop's IT systems they would have a way to install malware on the terminals to start pilfering credit card information.

The researchers provided *Forbes* with an image showing they'd fully compromised a Verifone terminal to display whatever they wanted.



A Verifone device is hacked for Forbes. Patches should prevent real-world attacks. TIMUR YUNOSOV

Disclosure to Verifone and Ingenico started two years ago and the issues have now been patched, according to the vendors. Both companies said the attacks were limited, given the need for physical access and prior research to hack into them.

MORE FROM FORBES ADVISOR

Best High-Yield Savings Accounts Of September 2023

By **Kevin Payne** Contributor

Best 5% Interest Savings Accounts of September 2023

By **Cassidy Horton** Contributor

A Verifone spokesperson said the affected devices were “legacy” and the company was not aware of the vulnerabilities being exploited by real-world hackers.

“The security firm has validated that our latest patches and software updates, which are available to all customers, remedy these vulnerabilities. Customers are currently in different phases of implementing these patches or software updates,” a spokesperson added.

An Ingenico spokesperson said: “Different vulnerabilities impacting Ingenico POS Telium 2 terminal solutions have been identified. Proper security measures have been developed immediately to include suitable corrections after the vulnerabilities have been identified.

“Ingenico has not been made aware of any fraudulent access to payments data resulting from these vulnerabilities, already fully

corrected." They added the company "is closely monitoring the situation to avoid reoccurrence of this issue."

Follow me on Twitter. Check out my website. Send me a secure tip.

Thomas Brewster

Follow

I'm a senior writer for Forbes, covering security, surveillance and privacy. I'm also the editor of The Wiretap newsletter, which has... **Read More**

Editorial Standards

Reprints & Permissions