Risk Management | Data Security

September 23, 2009

POS PIN Entry Device Vulnerabilities

Compromised point-of-sale (POS) PIN-entry devices (PEDs) equipped with tapping mechanisms designed to capture PIN and card data have recently been found in the U.S. marketplace. Visa clients must take action to mitigate the risks introduced by these compromised POS PEDs.

POS Vulnerabilities

Visa has received an increasing number of reports regarding POS PED thefts from merchant store locations. Evidence indicates that POS PEDs are being physically removed from their locations and replaced with modified devices designed to skim account and PIN data. Surveillance has shown that suspects in most of these cases were able to remove and install a POS PED in under one minute. This type of fraud typically occurs in merchant locations with “after-hours” operations where there is minimal customer traffic or employee supervision over cash registers.

Merchant locations targeted include supermarkets, drug stores and convenience stores; however, any store may be affected by this scheme if older POS PEDs that are not tamper-evident or tamper-resistant are in use. PEDs targeted by criminals include:

- **VeriFone**: PINpad 101, 201 and 2000
- **VeriFone**: Everest model P003-3xx
- **Hypercom**: S7S and S8
- **Ingenico**: eN-Crypt 2400 (also known as the C2000 Protégé)

These POS PEDs were deployed prior to Visa’s implementation of a POS PED testing program and must be removed from production by **July 1, 2010**. Their vulnerabilities have been communicated to acquirers through articles published in the *Visa Business News* and in *Security Alerts* published on www.visa.com/cisp.

For more information on the mandatory retirement requirements for these vendor-attested attended POS PEDs, please review the *General PED Frequently Asked Questions* document available on www.visa.com/pin.

Ingenico: eN-Crypt 2100

The most recently identified attended POS PED, the Ingenico: eN-Crypt 2100, is a pre-PCI approved device[1] that expired on December 31, 2007. Entities are encouraged to retire this recently identified compromised POS PED as quickly as possible. Soon, Visa will announce a sunset date for all attended pre-PCI POS PEDs.

Related Information

Visa Business News Archive

Key Dates

Visa Online

Recommended Mitigation Strategies and Best Practices

Visa strongly recommends that merchants use heightened vigilance and maintain a secure store environment at all times, especially around cash registers and POS PEDs. Visa recommends the following best practices:

- Merchants should have the ability to monitor PED internal serial numbers and detect when PED serial numbers change or if a PED is disconnected or removed.
- Merchants must ensure that only authorized personnel service deployed terminals and PEDs in accordance with *Payment Card Industry PIN Security Requirements*. (See www.visa.com/cisp for more information.)
- Merchants must properly manage PED inventories and physically secure PEDs at all locations so PEDs cannot be easily modified or replaced.
- Merchants are advised to purchase only PCI-approved PEDs that have been lab-evaluated.

Visa U.S.A. Inc. Operating Regulations and Interlink Network, Inc. Bylaws and Operating Regulations require that PEDs deployed by members and their agents comply with the *Payment Card Industry PED Security Requirements*. As of January 1, 2004, newly purchased attended POS PEDs from original equipment manufacturers must be Visa-approved and lab-evaluated. To review Visa global PED testing requirements, clients should refer to the *PCI PIN Security Requirements, Appendix A*, available at www.visa.com/cisp.

Visa/Interlink merchants must only deploy PEDs listed on the *Payment Card Industry PIN-Entry Device Approval List* found at www.pcisecuritystandards.org/pin. Clients must ensure that all PEDs purchased use the exact PED identifier, make, model and firmware version provided on this list.

Visa is aware that non-approved PED acquisitions are still occurring. Entities that deploy non-compliant devices are in violation of Visa PED deployment mandates and may be found liable in the event of a PIN compromise.

Merchants are encouraged to work with their merchant bank and/or Encryption and Support Organization (ESO) to create a plan to ensure that all deployed POS PEDs are PCI-approved and comply with Visa Triple Data Encryption Standard (TDES) requirements. (See the April 22, 2009, *Visa Business News* article entitled, “Update on Visa’s Compliance Policy to Facilitate Triple Data Encryption Standard Usage.”)

Merchants should train their employees on the potential for PIN compromise and what actions to take if a POS PED is stolen or missing, or there are noticeable signs of device-tampering. Merchants are also advised to inspect POS PED inventories regularly. If POS PED tampering is suspected, merchants should immediately contact their merchant bank, Visa, and law enforcement. To build awareness of emerging vulnerabilities, acquirers may share this bulletin with their merchants, agents and other parties, and encourage all parties to take steps, where appropriate, to mitigate risk.

Attend PIN Security Training on October 7, 2009

To support compliance with the *Payment Card Industry PIN Security Requirements*, Visa is committed to helping clients, merchants and payment system participants better understand their responsibilities related to securing PIN data. To aid client and merchant compliance efforts, Visa provides ongoing educational PIN Security training

to help entities gain further knowledge in all aspects of secure key management.

The next one-day Visa Key Management Training will be held in Foster City, CA, on October 7, 2009. For training and registration information, please go to www.visa.com/cisp or e-mail pinusa@visa.com for more information.

[1] A device that was designed and tested earlier than PCI PED version 1.x specifications.

Related Documents

Additional information on PED Security, the *Payment Card Industry PIN Security Requirements* and TDES can be found in the following Visa publications and on Visa and Payment Card Industry websites:

"Information Supplement: Skimming Prevention – Best Practices for Merchants" Payment Card Industry Security Standards Council, August 2009.

"Visa PIN Security Tools and Best Practices for Merchants" brochure (Document Number: VRM 04.12.06)—Visit www.visa.com/pin or contact the Visa Fulfillment Center at (800) 235-3580.

"Payment Card Industry PIN Security Requirements" manual—Visit www.visa.com/pinsecurity or www.visa.com/cisp or the "PIN Security" section of Visa Online.

"General PIN Entry Device Frequently Asked Questions"—Visit www.visa.com/pin.

"Payment Card Industry PIN-Entry Device Approval List"—Visit www.pcisecuritystandards.org/pin.

"Update on Visa's Compliance Policy to Facilitate Triple Data Encryption Standard Usage," *Visa Business News*, April 22, 2009.

"PIN Pad Found Vulnerable to Skimming Attacks," *Visa Business Review*, Issue No. 070327, March 27, 2007.

"Members Are Reminded that POS PIN Pads Susceptible to Skimming Attacks Must Be Replaced", *Visa Business Review*, Issue No. 070313, March 13, 2007.

"Visa Requires Laboratory Testing of PIN-Entry Devices," *Visa Business Review*, Issue No. 030527, May 27, 2003.

"Visa Announces Initial Triple DES Implementation Requirements," *Visa Business Review*, Issue No. 020813, August 13, 2002.

For More Information

For more information or questions, please email pinusa@visa.com.