Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India

CERT-In Advisory CIAD-2016-0062

Security of POS Systems

Original Issue Date: November 27, 2016

Systems Affected

- Point of Sale Systems

Description

The point of sale (POS) is the place where a retail transaction occurs and the merchant calculates the amount owed by the customer, indicates the amount, prepares an invoice for the customer, and indicates the options for the customer to make payment. It is also the point at which a customer makes a payment to the merchant in exchange for goods or after provision of a service. After receiving the payment, the merchant issues a receipt for the transaction, which is usually printed, but is increasingly being dispensed with by sending it electronically.

POS systems consist of hardware as well as software that tells the hardware what to do with the information it captures. When consumers use a credit or debit card at a POS system, the information stored on the magnetic stripe of the card is collected and processed by the attached device. The data stored on the magnetic stripe is referred to as Track 1 and Track 2 data. Track 1 data is information associated with the actual account and it includes items such as the cardholder¿s name as well as the account number. Track 2 data contains information such as the credit card number and expiration date.

Threats to POS Systems

1. Skimming

Skimming is an electronic method of capturing a victim's personal information used by identity thieves. The skimmer is a small device that scans a credit/debit card and stores the information contained in the magnetic strip. Skimming can take place during a legitimate transaction at a business.

2. POS Malware

Point-of-sale malware (POS malware) is a type of malicious software (malware) that is used by cybercriminals to target point of sale (POS) terminals with the intent to obtaining credit card and debit card information by reading the device memory from the retail checkout point of sale system.

Best Practices

Owners and operators of POS systems should follow best practices to increase the security of POS systems and prevent unauthorized access.

For organisations / service providers:

- Update POS Software Applications: Keep all POS Systems regularly updated including POS application software.
- Use Antivirus: It is suggested to continually update the antivirus programs for it to be effective on a POS network.
- Install a Firewall: Firewalls should be utilized to protect POS systems from outside attacks. A firewall can prevent unauthorized access to, or from, a private network by screening out traffic from hackers, viruses, worms, or other types of malware specifically designed to compromise a POS system.
- Restrict Access to Internet: Apply access control lists on the router configuration to limit un authorized traffic to POS devices.
- Disallow Remote Access: Cyber Criminals can exploit remote access configurations on POS systems to gain access to these networks. To prevent unauthorized access of POS systems, disallow remote access to the POS network at all times.
- Review all Logs: Organizations and merchants providing POS services should review all system logs for any strange or unexplained activity on a regular basis.
- Encrypt transmission of card holder data across open, public network .

For Merchants:

- Update POS Software Applications: Keep all POS Systems regularly updated including POS application software.
- Review all Logs: Organizations and merchants providing POS services should review all system logs for any strange or unexplained activity on a regular basis.
- Account Lock out policy: Locking out accounts after N number of incorrect login attempts.
- POS systems should not be used for general internet access by retailers.
- Use Strong Passwords: All POS devices owners should change passwords to their POS systems on a regular basis, using unique account names and complex passwords.
- Merchants should ensure that all their Wi-Fi and internet connections are secured. Merchants may use a network name that is extremely generic but unique keeping the network simple and inconspicuous. In addition Merchants may modulate the signal strength of their Wi-Fi network so that it does not extend

too far from the area of use or shop or building.
- Ensure that no electronic / magnetic devices are attached with POS systems. Enter the PIN numbers in a secret manner.
- Merchants should always purchase POS Systems from reputable dealers.
- If any suspected transactions are observed, contact the service provider / bank immediately.

References

https://www.us-cert.gov/ncas/alerts/TA14-002A
https://www.sans.org/reading-room/whitepapers/bestprac/point-sale-pos-systemssecurity-35357
https://www.symantec.com/content/dam/symantec/docs/white-papers/attacks-on-point-of-sale-systems-en.pdf
https://erply.com/5-tips-to-protect-your-retail-business-against-security-breaches
http://whatis.techtarget.com/definition/point-of-sale-security-POS-security

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.

Contact Information

Email: info@cert-in.org.in
Phone: +91-11-24368572

Postal address

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,
New Delhi - 110 003
India