Visa Data Security Alert

Top Vulnerability—Packet Sniffing

February 2, 2009

To promote the security and integrity of the payment system, Visa is committed to helping clients and payment system participants better understand their responsibilities related to securing cardholder data and protecting the payment industry. As part of this commitment, Visa issues Data Security Alerts when emerging vulnerabilities are identified in the marketplace, or as a reminder about best practices.

Clients may share this alert with their stakeholders to ensure that they are aware of these emerging vulnerabilities and take steps to mitigate risks.

Packet Sniffing Vulnerability

Visa originally published this data security alert in January 2008. This update reflects the latest information from forensic investigations of data security breaches indicating an increasing prevalence of packet sniffers designed to intercept and collect cardholder data.

Packet sniffing is the practice of using computer software or hardware to intercept and log traffic passing over a computer network. A packet sniffer, also known as a network analyzer or protocol analyzer, captures and interprets a stream or block of data (referred to as a "packet") as it travels over a network.

Recent compromises have involved the use of packet sniffers installed on systems with access to cardholder data. Criminals used sniffer software programs to steal cardholder data from transactions passing through the compromised entity's computers. Additionally, recent investigations have uncovered evidence of packet sniffers being used by network intruders to capture payment card data as it is transmitted over the network during authorization. This threat involves compromising the system and then installing a sniffer software program. These sniffers may have the capability to search specifically for cardholder data and then write the data to a file so it can be collected later by criminals.

While there are legitimate uses for sniffing such as maintaining networks (e.g., analyzing network problems, monitoring network usage or testing firewalls), sniffing is also used to gain information that can enable network intrusion or identity theft.

Packet sniffers are a form of malicious software or "malware." Once network intruders gain entry into a processor, service provider or merchant's system, packet sniffer programs are installed and can be difficult to detect. Intruders can then "sniff" packets being sent between network users, and can collect sensitive information such as usernames, passwords, payment card data or social security numbers. This malware is effective in compromising systems and networks because sniffers are invasive and difficult to detect by design.

Recommended Mitigation Strategy

Although packet sniffing is difficult to detect, steps can be taken to mitigate the risk of exposure to critical systems such as point-of-sale (POS) systems, payment processing servers, database servers or other servers where cardholder data is stored and transmitted. To get started, follow these best practices:

- Utilize an automated tool/process to regularly scan for stored cardholder data that was unauthorized or unprotected
- Utilize host-based Intrusion Detection Systems (IDS)
- Monitor firewalls and logs for suspicious traffic/activities, particularly outbound traffic to unknown addresses
- Alert and prevent cardholder data from unknowingly leaving the network
- Implement file integrity monitoring
- Secure workstations so packet sniffers or other malware cannot be installed
- Utilize encrypted protocols or encryption to protect sensitive data
- Use packet sniffers legitimately to detect network intrusion attempts or suspicious activity on a network
- Ensure that anti-virus and anti-spyware software programs are up-to-date
- Routinely examine systems and networks for newly-added hardware devices
- For users and applications, implement the least privileges necessary

For more information or questions regarding the information in this alert, please visit www.visa.com/cisp or e-mail cisp@visa.com.