

Visa Data Security Alert

Packet Sniffing Vulnerability

January 31, 2008



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 help ensure they are aware of these emerging vulnerabilities and take steps to mitigate risks.

Packet Sniffing Vulnerability

Visa has seen an emerging trend of computer hackers using packet sniffers 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") traveling over a network.

Some recent compromises involved the use of packet sniffers installed on critical systems. Criminals used sniffer programs or hardware to steal card 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 track data as it is transmitted over the network during authorization. The threat involves compromising the system by installing a sniffer program or installing a hardware sniffer. These sniffers are then used to collect cardholder data.

Although sniffing has legitimate uses in maintaining networks (i.e., analyzing network problems, monitoring network usage or testing firewalls), its used to gain information that enables a network intrusion or identity theft, has made it a significant threat.

Packet sniffers are typically used in conjunction with malicious software or "malware." Once network intruders gain entry into a critical system using backdoor programs or deploying rootkits, the sniffer programs are installed, making the malware more difficult to detect.

Intruders can then "sniff" packets between network users and collect sensitive information such as usernames, passwords, payment card data or social security numbers. Once a critical system or network is compromised, sniffers are used to eavesdrop or spy on network users and activity. This combination of tools makes this attack scheme quite effective in compromising systems and networks.

Recommended Mitigation Strategy

Although packet sniffing is difficult to detect, the following best practices should be utilized 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 resides:

- Utilize host based Intrusion Detection Systems ("IDS")
- Monitor firewalls for suspicious traffic, particularly outbound traffic to unknown addresses
- 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 anti-virus and anti-spyware software are up-to-date
- Routinely examine systems and networks for newly added hardware devices

For more information and mitigation strategies regarding data security vulnerabilities, please visit www.visa.com/cisp to download the *Potential Network Vulnerabilities for Financial Institutions* alert.

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