



MICROS SYSTEMS, INC. SECURITY ADVISORY

APRIL 21, 2009

To All Valued MICROS Customers:

We are publishing this advisory today in an ongoing effort to continue to inform all of our MICROS customers of security issues, and to address various inquiries we have recently received in connection with the October 2, 2008 Visa Data Security Alert titled “Debugging Software – Memory Parsing Vulnerability”.

Immediately after Visa issued its Visa Security Alert on October 2, 2008, MICROS commenced a comprehensive security investigation, conferring with Visa, the MICROS Research and Development teams, and Trustwave, an independent and PCI-SSC certified Qualified Security Assessor. The two issues analyzed were as follows:

- a. Were any of the 19 MICROS payment application products (both restaurant and hotel) vulnerable to the type of attack identified in the Visa Security Alert; and
- b. Were any enhancements to the MICROS payment applications necessary to address this new threat?

After investigation, it was conclusively determined that no MICROS applications were hacked or infected with the malware, and accordingly there is no need to modify any of the MICROS applications. It is important to understand, however, that Visa has determined that certain merchant networks were infected with malware, which extracted unencrypted cardholder data **before** it was encrypted by the payment processing application, including MICROS payment processing applications. Merchants with relaxed network security are susceptible to this type of attack. The attackers typically gain access to the Merchant network because the Merchant is using default or generic user names and weak passwords that are easy to break, incorrectly configured firewall or no firewall, flat network topology, open communications ports, and poorly configured remote access tools. After the attacker gains access to the Merchant’s network, the malware is then installed and sensitive unencrypted cardholder data is extracted from the volatile operating system memory, and not the payment processing application. Accordingly, a merchant could be using a PABP or PA-DSS validated payment processing application, including MICROS products, and still have credit card data stolen using this method of attack. However, a merchant whose system is fully PCI-DSS compliant (which includes both network security features and a PABP or PA-DSS validated product, such as those offered by MICROS) is not vulnerable to such attack. Merchants using any and all payment processing applications are subject to this attack, even if they are using a PABP or PA-DSS product. According to the Verizon Business 2009 Data Breach Investigations Report, malware was involved with over one-third of compromise investigations and contributed to 9 out of every 10 records breached.

Page 1 of 2



Furthermore, Verizon Business saw an increase of 641% in compromised records over the previous year. This method of attack is clearly on the rise. It is our understanding that Visa will soon issue an additional alert to highlight the sensitivity of this matter and the increasing number of attacks.

Nicholas Percoco, Vice President and head of Trustwave's Spider Labs, which contains a forensic investigations unit, stated: "As the PABP and PA-DSS payment applications have become more robust and secure, attackers are no longer able to extract unencrypted cardholder data from these validated applications while the data is in transit or being stored. Therefore, the attackers are modifying their techniques. The type of malware attack identified in the Visa security alert extracts restricted cardholder data from volatile operating system memory, which the PABP or PA-DSS validated payment applications do not control. This malware is not directed towards any specific payment application. The recommended mitigation strategy for Merchants is to secure their networks and operating system by complying fully with the Payment Card Industry Data Security Standard (PCI-DSS)."

Additionally, MICROS conferred with representatives from Visa, who concurred that the correct Merchant mitigation strategy for this type of attack is to comply with the terms of the PCI-DSS, in order to prevent the attackers from accessing the Merchant network and installing this type of malware. For more information on the PCI-DSS, please refer to the following link:

https://www.pcisecuritystandards.org/security_standards/pci_dss_download_agreement.html

In October 2008, MICROS posted (and continues to post) a link to the Visa Security Alerts on the Information Security section of the MICROS web site. MICROS will continue to post relevant security information on its website as new information becomes available. To access the Visa Security Alerts, please refer to the following link:

http://usa.visa.com/merchants/risk_management/cisp_alerts.html

Thank you.