Verifone SECURITY ADVISORY

MX900 Series Potential Vulnerability **July 27, 2017**

Verifone works collaboratively with the industry, our clients and security experts to ensure the continued security of the payments system. As part of this effort, we have recently learned of a potential vulnerability impacting MX900 series products running on older versions of the device's operating system. To exploit this vulnerability requires physical access to the device and existing knowledge of its password. It was identified in a lab by a security researcher who has not shared the specifications publicly, and there are no reported issues in the field.

This vulnerability is affects all MX900 Series devices OS versions 30145200 or earlier than. Clients running these older OS versions can significantly reduce their exposure by following these best practices:

- Ensure all default passwords are changed and updated regularly
- For devices running OS 20120625 or 30145100, clients should upgrade to the latest OS and install the security patch that will be available next week.
- For devices running OS 30140200 or 30145200, clients should install the security patch that will be available next week.
- For all MX900 Series devices, clients should develop a plan to update their devices to the latest OS as soon as reasonable. Verifone continuously works to upgrade the features and security of our operations systems, and this vulnerability has already been mitigated through additional hardening and changes to the API in latest OS version, which also includes additional bug fixes and other enhancements.
- Implement a device management solution that tracks the location of each device, and alerts personnel when devices are removed, replaced or added without prior authorization and provides for an easy mechanism for firmware updates

Additionally, Verifone recommends the following best practices to ensure optimal device security:

- Secure devices in a locking stand
- Store spare devices under lock and key to prevent unauthorized removal
- Track when devices are replaced within the store, whether from in-store inventory, by a repair technician, or with units shipped into the store
- Require all repair technicians who visit your stores to sign in, to verify their identity with photo identification, and to remain accompanied by store personnel during any work on payment devices
- Install locking stands to prevent unauthorized device removal
- Use only authorized vendors for device acquisition and repair

Verifone takes all threats to the payments system seriously. We have collaborated with this individual to understand his findings and – although his learnings were already addressed through routine OS upgrades – we are committed to doing whatever is necessary to keep our clients safe and secure. We would be more than happy to schedule a call with our security team if you have any concerns.