

ATM SECURITY CRITICAL UPDATE

LEVEL: URGENT

ATM Type: Diebold automated teller machines (ATMs) with a Windows®-based operating system.

SECURITY THREAT

Criminals have attempted to intercept sensitive information entered into Diebold ATMs that utilize a Windows®-based operating system. This crime involves physical access to the inside of the ATM and is not a network-level security compromise. This incident has been isolated in Russia, and the suspects have been apprehended. Diebold is working with law enforcement to assist with the investigation into these recent crimes.

SECURITY ISSUE

Diebold has been made aware of recent physical break-ins into a number of its Windows®-based ATMs in Russia. Criminals gained physical access to the inside of the affected ATMs. This criminal activity resulted in the operation of unauthorized software and devices on the ATMs which was used to intercept sensitive information. Diebold has determined this risk is significantly increased if the Windows® administrative password has been compromised, the hardened version of the Windows® operating system provided by Diebold is not used, or if the Sygate/Symantec firewall software provided with Diebold Agilis software has been disabled or is not properly configured.

RECOMMENDATIONS

Diebold is taking the precaution of providing a security software update that addresses this risk and recommends it be installed on all its Windows®-based ATMs globally. You will be contacted shortly by your Diebold representative to schedule installation of this update. Bringing the ATM software to current levels should be sufficient to prevent the attacks that have recently been attempted.

Any Diebold Windows®-based ATM on which the default Windows® password has not been changed or on which a secure password change has not been recently made, should have the password changed. A process for secure periodic changes to the Windows® administrative password should be implemented. ATMs should also have the Windows® desktop disabled.

The Sygate/Symantec firewall software provided with Diebold Agilis software should be operational and should be configured to assure that the ATM may only communicate with authorized system addresses. Diebold Windows®-based ATMs that do not have a Diebold hardened Windows® operating system installed should be modified to reduce risks of unauthorized access.

HOW TO OBTAIN FURTHER INFORMATION

If you have questions concerning this ATM security update, or require assistance to reduce the risk of criminal attack against your ATMs, please contact atmsecurity@diebold.com. It is strongly recommended that customers register for Diebold software update notifications from Diebold Customer Internet Support at <http://www6.diebold.com/support/notification/>.