Technical Bulletin - RMS Attack - Mar 5, 2025

Valued Customers,

Hyosung has received multiple reports of active RMS attacks in the marketplace that are focused on outdated ATM software. Hyosung strongly recommends shutting down MoniView (see instructions below) until all your machines are upgraded to WinCE 6.3.10 (or later). The latest software prevents the attacks we are currently witnessing. Please take the following actions:

1. Temporarily close the MoniView port (9998, 9999) on your firewall to prevent ATMs from reaching your MoniView server.
2. Disable the MoniView Service (Launch C:\Nautilus Hyosung\MoniView\MoniView.ServerManager.exe - click Stop under "MoniView Server Service").
3. Disable the SQL Server Service.
4. Perform a port scan on your public IP to ensure that:
   a. Ports 9998 and 9999 are temporarily closed.
   b. 1433 and 9000 are closed – these should never be open to the internet.

Hyosung also recommends you work with your communications provider to whitelist only your current RMS and Host IP addresses and prevent ATMs from reaching rogue RMS and Host IP addresses.

Sincerely,

Keith Lennard

Executive Vice President

For more information please refer to our Software Support Customer Portal Documentation

If you have any questions, please contact us at 1-877-Hyosung.