HYOSUNG TNS Technical Bulletin

Technical Bulletin #HTB-2025-004: DMA Attack Alert and Mitigation

Issued: 2025-06-26

Subject: DMA Attack Alert and Mitigation Recommendations for Hyosung ATMs

To Our Customers,

Hyosung TNS is issuing this Technical Bulletin to alert you to recent Direct Memory Access (DMA)-based attacks targeting ATMs and to provide actionable recommendations to mitigate these threats.

Incident Overview

In May 2025, industry security and field reports confirmed DMA-based attack attempts on ATMs in regions of South America. Attackers gained physical access to the ATM's internal system, connecting a malicious device (e.g., a Raspberry Pi) to exposed PCIe interfaces to inject malicious DLL files into the file system. While no successful cash manipulation has been reported on Hyosung ATMs, these incidents underscore the need for heightened security measures to prevent potential data or system compromise.

Mitigation Strategies

We share the following strategies to protect your Hyosung ATMs from DMA-based attacks.

1) Prevent Malicious DLL Execution

If using BlueVerseSecurity (a trusted ATM security solution), ensure policies are configured to block unauthorized DLL execution. Contact Hyosung for configuration assistance.

2) Restrict Direct Memory Access

For ATMs running Windows 10/11 with compatible hardware (e.g., Input Output Memory Management Unit—IOMMU), the Kernel DMA Protection feature can restrict unauthorized DMA by peripheral devices. Hyosung is planning a comprehensive project to support DMA restrictions across various Hyosung ATM configurations as follows:

- For later environments (Windows 10 version 2019 or later): Update BIOS to enable Kernel DMA Protection.
- For earlier environments (Windows 10 version 2016 or earlier): Custom build BIOS to deactivate targeted PCIe ports, preventing unauthorized device connections.

Call to Action

To safeguard your Hyosung ATMs, we urge you to:

- Verify your BlueVerseSecurity settings immediately.
- Contact Hyosung to discuss BIOS update requirements.

We are committed to supporting you in maintaining the security and integrity of Hyosung ATMs. For assistance, please reach out to your regional support representative.

Sincerely,

Boick Chang (boick.chang@hyosung.com)

Head of Software Development

Hyosung TNS