HYOSUNG TNS Technical Bulletin

Technical Bulletin #HTB-2026-001: DMA Attack Alert and Mitigation

Issued: 2026-02-10

Subject: DMA Attack Alert and Mitigation Recommendations for Hyosung ATMs

To Our Customers,

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

DMA Attack Overview

Industry security and field reports have alerted to and confirmed DMA-based attack attempts on ATMs. Attackers gain physical access to the ATM's internal system and connect a malicious device (e.g., a Raspberry Pi) to exposed PCIe interfaces to inject malicious DLL files into the file system. These evolving threats underscore the need for heightened security measures to prevent potential data or system compromise.

Mitigation Strategies: Restrict Direct Memory Access

The Kernel DMA Protection feature can restrict unauthorized DMA access from peripheral devices in ATMs running Windows 10/11 with compatible hardware (e.g., Input/Output Memory Management Unit—IOMMU). Accordingly, Hyosung has mitigation solutions 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 with **no** Kernel DMA Protection feature): **Custom build BIOS** to deactivate targeted PCIe ports, preventing unauthorized device connections.

Call to Action

To safeguard your Hyosung ATMs, we urge you to contact Hyosung to discuss the requirements for a BIOS update or a custom build.

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