NUSOURCE

# NuSource Security Update

- **Bulletin: DMA Attacks – U.S. Activity Confirmed**
- **Issued: Sept 2nd, 2025**
- **Updated: Dec 22nd, 2025**

## Overview

**NuSource is now observing attack activity within the United States that is similar in nature to the Direct Memory Access (DMA) attacks previously reported in South America.**

These attacks require physical access to the terminal and involve connecting unauthorized devices (such as small single-board computers) to exposed PCIe or internal ports to inject malicious files directly into system memory.

## Short-Term Mitigation Options

**Through-the-Wall Terminals**

- New Barrel Key and Lock – Source the lock and key through a local locksmith to get the lock for each manufacturer and have them keyed alike.
- CCTV – Suspicious Activity or Loitering Notifications

**Free-Standing Island Terminal**

- New Barrel Key and Lock – Source the lock and key through a local locksmith to get the lock for each manufacturer and have them keyed alike.
- Security Gate – To gain access to the top hat, one must first open the ATM beauty door. The Security Gate should prevent unauthorized individuals from opening the beauty door and gaining access to the top hat.
- Install Hood Contact
- Alarm Top Hat
- Audible Siren
- CCTV – Suspicious Activity or Loitering Notifications

**Free-Standing Lobby Terminal**

- New Barrel Key and Lock – Source the lock and key through a local locksmith to get the lock for each manufacturer and have them keyed alike.
- Install Hood Contact
- Alarm Top Hat
- CCTV – Suspicious Activity or Loitering Notifications

NUSOURCE

## Long-Term Remediation Strategy

To address attack techniques similar in nature to those previously observed in South America, which rely on physical access and low-level system interaction, NuSource recommends the following long-term security measures:

**Upgrade or Replace ATMs to Support Windows 10 (2019/2021)**

- During Windows 10 (2019/2021) and Windows 11 upgrade projects,
  - BIOS passwords will be changed, and Kernel DMA Protection will be enabled.
  - All newly staged terminals are deployed with updated BIOS passwords and Kernel DMA Protection enabled by default.

NuSource can assist customers in evaluating their current hardware and operating system levels and in developing an upgrade or replacement strategy aligned with long-term security and operational goals.

## Our Commitment

NuSource is actively monitoring evolving attack methods and taking immediate action to protect your ATM/ITMs. For additional questions about ATM/ITM security, please contact your NuSource representative. They will ensure you have everything you need to protect your terminals against all known attacks.