NUSOURCE

NuSource Security Update

- **Bulletin: DMA Attacks**
- **Issued: Sept 2nd, 2025**

Overview

Recent reports confirm Direct Memory Access (DMA) attack attempts on ATMs in South America. Attackers physically connect devices (e.g., Raspberry Pi) to exposed PCIe interfaces to inject malicious files.

No successful attacks have been reported on Hyosung ATM/ITMs, but NuSource is proactively strengthening protections to safeguard our customers.

What NuSource Is Doing

• Securing BIOS: Kernel DMA Protection will be enabled in BIOS on all supported cores running Windows 10 2019 and later. Kernel DMA Protection is not supported on cores running Windows 10 2016. Additionally, BIOS passwords will be updated remotely on terminals with supported cores to restrict unauthorized access.
• Windows 10 (2019/2021) and Windows 11 Projects: Changing BIOS passwords, enabling Kernel DMA Protection on all cores during upgrades.
• New Terminals: All new terminals are staged with a new BIOS password and Kernel DMA Protection enabled.

What Customers Should Do

Contact your NuSource representative to determine if you're your machines are protected.

- Does your terminal support remote BIOS updates? Not all cores support them. If your machine does not, NuSource can help you develop a plan.
- What steps can you take to ensure Kernel DMA Protection can be enabled on your terminals?

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.