P25-14/0003 – Direct Memory Access (DMA) Attack

20250422/DS/01 **April 22, 2025**

Summary

Diebold Nixdorf (DN) has recently become aware of a successful malware-based jackpotting attack via Direct Memory Access (DMA) in Mexico on Opteva 522 terminals. Attackers gained access to the top chassis of the ATM, broke into the computer housing and installed a foreign Peripheral Component Interconnect Express (PCIe) device into the PCIe slot of the system. The PCIe device was used to interact with the Random Access Memory (RAM) of the target system. In general, a DMA attack can occur on a variety of systems, regardless of the system type, the manufacturer and the industry.

Description of Attack

High-speed expansion ports, like PCIe, utilize DMA to read/write the memory of a computer component or system's Central Processing Unit (CPU). DMA is used to increase performance of data transfers used by standard technologies such as PCIe, Firewire, Thunderbolt, PCMCIA, CardBus, or Expresscard. This document focuses on DMA capable PCIe devices, as the other above-mentioned ports are not part of the standard delivery of Diebold Nixdorf PCs. Some of these interfaces are already obsolete.

Apart from the legitimate use cases, DMA can potentially be used to bypass security controls of the terminal and illegitimately gain access and/or manipulate sensitive information in the terminal's memory. A DMA-capable device could be used to perform a variety of unauthorized actions, including mounting the filesystem, copying files, manipulating user passwords and/or execution of foreign executables and payload.

In the reported incident, attackers gained physical access to the computer chassis and installed a foreign DMA capable device into the PCIe slot of the system. This device was interfaced with an external device, which executed commands leading to unauthorized cash dispenses.

Recommendation for Countermeasures

Due to the architecture of DMA, traditional logical countermeasures like antivirus are not able to deter direct access to system memory via hardware interfaces.

To deter cyber-attacks on self-service terminals, DN recommends all customers implement a layered approach utilizing a combination of hardware and software security controls as well as monitoring and organizational countermeasures. For comprehensive details on countermeasures against jackpotting, please refer to the related fACT Sheet (20230616 FACT SHEET Jackpotting).

As stated above, it is highly recommended to implement a layered approach holistically protecting the terminal against DMA as well as Jackpotting attacks:

1) Deactivation of unused ports

- Limit logical access by disabling unused ports in the BIOS of the terminal's computer.
- Limit physical access to unused ports on the ATM computer by physically blocking them.

2) Implement Hardening of the Software Stack

- Introduce intrusion prevention mechanisms to identify deviating system behavior and protect the terminal during operation (online attacks). This does not protect against the execution of DMA itself but may alleviate the impact.
- In particular, the security solution should protect the XFS interface against unauthorized usage.
- Block the installation of foreign devices by using Windows Group Policies.
  Note: The activation of Windows Group Policies only applies to devices that have not been installed on the system yet. A device that was installed before the activation of the Windows Group Policies will still function as designed.
- Deploy a hardware-dependent hard disk encryption.

3) Microsoft Kernel-DMA Protection

- Microsoft implemented Windows internal security measures for kernel DMA protection. First introduced in Windows 10 1803 or LTSC 2019, these features leverage the system Input/Output Memory Management Unit (IOMMU) to block most DMA capable devices from accessing arbitrary memory segments.
- For more information and limitations on Microsoft's Kernel-DMA Protection, please refer to the official documentation from Microsoft.

4) Limit Physical Access to the Terminal

- Use appropriate locking mechanisms to secure the head compartment of the terminal.
- Control access to areas used by personnel to service the terminal.
- Implement access control for service technicians based on two-factor authentication.
- Terminal operators should conduct frequent visual inspections of the terminal.
- Consider adding physical protection with the DN Series Chassis Enforcer Package to harden the ATM top chassis against forcible entry.

5) Set Up Additional Measures

- Ensure real-time monitoring of security-relevant hardware and software events including but not limited to deviating or non-consistent transaction, event patterns or interrupted connection to the host or internal devices, etc.
- Hardware events, such as the addition of new PCIe devices or unauthorized access to top chassis or PC housing, may indicate an attack. Software events, such as deviating or inconsistent transactions, event patterns or interrupted connections to the host or internal devices, could also help identify suspicious behavior.

In general, we highly recommend using solutions specific to self-service terminals.

For detailed information, please contact your local sales department, a hardware integration representative or your Diebold Nixdorf security expert.

Additional Information & Contact:

Diebold Nixdorf | Product & Solution Security
security@dieboldnixdorf.com

Check out the Diebold Nixdorf Security blogs:
Banking Insights | Retail Insights

Did someone forward you this document?
Subscribe now to receive ACTive Security Alerts