NCR ATM Security Alert

DATE: May 2022 **INCIDENT NO:** 2022-02 **REV:**

“BootHole” GRUB2 Vulnerability

Microsoft and Eclypsium, published the details of a vulnerability publicly on their respective advisories and blogs.

- Microsoft Advisory: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV200011
- Eclypsium Technical Disclosure Writeup: https://eclypsium.com/2020/07/29/theres-a-hole-in-the-boot/

Through these, Microsoft have also published an update to the Certificate Revocation List File – which they refer to as the “DBX Update”.

This post also includes the technical details which explain Microsoft’s recommended approach to apply the DBX update to the EFI Firmware of a machine by using PowerShell https://support.microsoft.com/help/4575994

What is the vulnerability?

There is a vulnerability in the GRUB2 bootloader which can be exploited to bypass Secure Boot, allowing malware to be installed. This is only applicable on machines that use UEFI boot (not Windows 7).

The vulnerable “GRUB2” bootloader can be dropped into place on any UEFI based machine to bypass Secure Boot and execute malicious code (as a boot kit) before the operating system loads.

In order to exploit this vulnerability an attacker requires either:

1. Physical access to hard drive OR
2. Administrator privileges in Windows

Encrypted Hard Disks/ Application Whitelisting/ Anti-virus solutions/ Locked down BIOS cannot protect against this vulnerability.

Machines affected

Any NCR machine that runs on NCR’s Windows 10 OEM is susceptible to this vulnerability whether or not GRUB2 is used.

Customers who do not use NCR’s Windows 10 OEM but who do use UEFI are also susceptible to this vulnerability whether or not GRUB2 is used.

Windows 7 customers are not impacted by this vulnerability however they are already vulnerable to boot kit attacks, as are customers who use Windows 10 without Secure Boot being enabled.

Actions needed to prevent exploitation of this vulnerability

Only applicable for Windows 10 ATMs/ITMs
SecureBoot must be enabled before applying this update.

Step 1

Customers should check with their technical build team/Linux distributer or vendor to determine if they use a version of GRUB2 which has not been patched for this vulnerability.

For customers who currently do use GRUB2, it must be replaced by a version which resolves the vulnerability prior to taking any of the other actions detailed here. If not replaced, any process that relies on this bootloader will no longer function. These versions will be dependent upon the version of Linux that is used so customers will need to contact their Linux distributer/vendor before proceeding to Step 2.

Customers who do not use GRUB2 should go straight to Step 2

Step 2

To prevent exploitation of this vulnerability the certificate that was used to sign the vulnerable GRUB2 bootloader must be revoked.

ALL customers (whether they use GRUB2 or not) must revoke this certificate. This is done by executing a Powershell script to revoke the certificate, which can be done using either a bootable USB or from Windows for remote execution.

Instructions for how to do this are available from Microsoft
https://support.microsoft.com/help/4575994

or

NCR can help perform this task. Please contact your NCR representative for details.