Dell EMC PowerEdge UEFI Secure Boot Customization: Reduce Attack Surface with Complete Control of Certificates

Introduction

While traditional datacenter security focuses on operating system, application, physical, and network levels, new evolving threats require specific attention to server firmware. Dell EMC servers include UEFI Secure Boot for firmware authentication and authorization. In addition to the standard UEFI Secure Boot customization capabilities for operating systems (OSs) and hypervisors (HVs), Dell EMC now offers full customization capabilities for I/O devices.

Dell EMC recognizes the risks in relying on standard UEFI Secure Boot signing keys currently used widely in the industry. For customers wanting to avoid standard keys, because of some of the risks they present, Dell EMC provides complete customization capabilities for UEFI Secure Boot, giving system owners an option to eliminate reliance on industry keys and industry certificate authorities.

Firmware Threats

An area of interest to malware developers is creating attacks on the server pre-boot environment. Firmware is stored in protected non-volatile storage and runs in privileged memory, separate from the operating system and storage media. Because of this separation, infected firmware can escape detection and remediation by both the operating system and antivirus software.

With direct access to hardware components via the firmware, those seeking to exploit a server can potentially compromise systems without the administrator’s knowledge, or detection by the operating system. When the system firmware is targeted, the compromise persists even if the hard drive is swapped out.

Absent use of Secure Boot, which prevents execution of unauthorized pre-boot code, firmware rootkits can compromise device or system firmware, or in the case of bootkits, alter the code path used to boot up the operating system. They can even survive re-installation of the operating system.
Reducing Risk with Standard UEFI Secure Boot

Legacy Basic Input/Output System (BIOS) interfaces present high-risk vulnerabilities and are being replaced with the Unified Extensible Firmware Interface (UEFI). PowerEdge servers supporting UEFI Secure Boot, an industry-wide standard for security in the pre-boot environment, check the cryptographic signatures of UEFI drivers and other code loaded prior to running the OS. These include OS boot loaders and UEFI drivers for PCIe cards and mass storage devices.

Secure Boot is a feature added to the UEFI specification version 2.3.1. The system administrator defines the Secure Boot policy, which the BIOS applies to pre-boot code modules. The BIOS uses the policy to determine whether to trust code modules. If any module does not satisfy the policy, the system BIOS neither loads nor executes the module.

The Standard Secure Boot policy contains industry-standard certificates that authorize all the third-party pre-boot firmware supported, such as OS boot loaders, hypervisors (HVs), and I/O devices, for that system. While the Standard Secure Boot policy provides a simple way to deploy UEFI Secure Boot, it still carries risk. The Standard policy authorizes many firmware binaries using only a few standard certificates. This broad authorization exposes the system to a broad set of potential vulnerabilities (such as the recent GRUB2 “BootHole” vulnerability, discussed further below).

Basic UEFI Secure Boot Customizations

Some system owners reduce the risks of the Standard Secure Boot policy by customizing the policy according to OS usage. For example, if a server is intended to boot only one OS, administrators remove certificates that authorize other OS(s). Other system owners, who develop custom OS components (kernels or boot loaders), sign the components with their own keys. In this case, the system owner replaces standard certificates in the policy with custom certificates. In this way, a Custom Secure Boot policy reduces risk by authorizing only specific OS boot loaders and HVs. Dell EMC servers support these basic customizations.

However, as shown in the figure above, such custom policies still include industry keys that trust a wide array of signed I/O device firmware. The UEFI CA certificate – part of the Standard Secure Boot policy – is used across the industry for authorizing I/O device firmware and “shim” (an early stage boot loader in Linux
distributions). Removing the UEFI CA certificate is desirable, but this presents some challenges since obtaining and custom-signing I/O firmware is difficult.

**Dell EMC’s Approach to Full Customization**

Dell EMC provides complete customization capabilities for UEFI Secure Boot, eliminating reliance on industry keys and industry certificate authorities. These capabilities include remote management tools for authorizing specific I/O device firmware and pre-boot binaries. Using these tools, system owners can customize their policy easily by removing the UEFI CA certificate and adding custom entries instead. A recent report from the U.S. Government’s National Security Agency (NSA) documents the topic of increased server hardware security, specifically citing the use of PowerEdge UEFI Secure Boot Customization as a method that provides a significantly higher level of security along with the flexibility to support multiple operating systems.

Note that Dell EMC enables removal of the UEFI CA certificate regardless of whether the system owner chooses to use their own public key infrastructure (PKI). System owners who maintain their own PKI rely only on custom policy entries (see the fifth level in the figure above). Other system owners, who do not maintain their own PKI, may choose to trust the OS vendor’s keys and still use Dell EMC’s approach to authorize specific I/O device firmware (see the fourth level in the figure above). In this way, system owners without their own PKI can still mitigate the risk of the UEFI CA certificate.

<table>
<thead>
<tr>
<th>Operating System Certificate</th>
<th>I/O Device Firmware Authorization</th>
<th>Is this configuration possible on Dell EMC servers?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft</td>
<td>Standard (UEFI CA)</td>
<td>✔ Yes</td>
</tr>
<tr>
<td>Microsoft</td>
<td>Customized</td>
<td>✔ Yes</td>
</tr>
<tr>
<td>VMWare / ESXi</td>
<td>Standard (UEFI CA)</td>
<td>✔ Yes</td>
</tr>
<tr>
<td>VMWare / ESXi</td>
<td>Customized</td>
<td>✔ Yes</td>
</tr>
<tr>
<td>Linux (UEFI CA)</td>
<td>Standard (UEFI CA)</td>
<td>✔ Yes</td>
</tr>
<tr>
<td>Linux (UEFI CA)</td>
<td>Customized</td>
<td>✔ Yes</td>
</tr>
<tr>
<td>Linux (Custom CA / PKI)</td>
<td>Standard (UEFI CA)</td>
<td>✔ Yes</td>
</tr>
<tr>
<td>Linux (Custom CA / PKI)</td>
<td>Customized</td>
<td>✔ Yes</td>
</tr>
</tbody>
</table>

Although complete customization requires careful management, this solution is attractive for system owners who want precise control over firmware authorization. When vulnerabilities are discovered in industry-signed firmware or industry-signed bootloaders, Dell EMC’s precise authorization method can help eliminate exposure, as in the case of the GRUB2 BootHole vulnerability.
GRUB2 BootHole Vulnerability

In July 2020, researchers disclosed a buffer overflow vulnerability in the GRUB2 Linux bootloader that enables arbitrary code execution in GRUB2. Dubbed “BootHole,” this vulnerability is significant because GRUB2 is normally launched by the “shim” early-stage bootloader, which is authorized by the UEFI CA certificate. Thus, attackers can modify the boot flow even when UEFI Secure Boot is enabled. The exploit is possible both on Linux and Windows systems.

Since Dell EMC servers offer complete customization of the Secure Boot policy – including removing the UEFI CA certificate – system owners can use customization to eliminate exposure to BootHole and similar classes of future vulnerabilities.

In Conclusion

Dell EMC UEFI Secure Boot Customization serves to minimize the attack surface in pre-boot firmware. Using custom Secure Boot policies, system owners fine-tune their firmware authorization rules, reducing exposure to potential vulnerabilities in industry-signed binaries.

Dell EMC PowerEdge is the first server vendor to provide advanced UEFI Secure Boot Customization, enabling customers to eliminate dependence on all third-party certificates and take full ownership of firmware execution. Using the precise authorization offered by Dell management tools, system administrators can optimize the effectiveness of their UEFI Secure Boot policy.