Dell Secure BIOS for PowerEdge 12th Generation Servers

A Dell technical white paper

Dell Server Engineering Team

Contents

Acknowledgements

This document references and/or includes material from the following sources:

- Direct2Dell Blog post "Securing Government IT From the Ground-Up" posted July 22, 2011
- National Institute of Standards and Technology Special Publication 800-147, "BIOS Protection Guidelines Recommendations of the National Institute of Standards and Technology"

June 2012

Executive summary

Malware and other cyber-security threats continue to multiply in the enterprise IT environment. Dell's own Counter Threat Unit (CTU) housed within Dell SecureWorks processes more than 13 billion security events a day and sees more than 30,000 specimen of malware a day. Security threats are almost literally everywhere, but sometimes system vulnerabilities can be found at even the most basic level.

BIOS firmware enables some of the most basic server functions through its unique and privileged position within the server architecture. From setting-up hardware and loading and starting an operating system, the functions this firmware supports are basic but also fundamental to the operation of any system, making them both easy to secure, but also vulnerable to attack.

Dell is constantly working to develop new and improved security features for our core server BIOS and iDRAC designs. For the past four server generations, we have offered digitally signed BIOS and iDRAC firmware updates. Also, we provide all updates (PSU, NIC, PERC, etc.) in DUP form in addition to BIOS and iDRAC. When sourced and deployed as recommended, these provide an extremely high level of protection for these important pieces of server firmware. For our newly introduced Dell PowerEdge 12th generation servers we have further enhanced this to incorporate BIOS protection guidelines currently recommended for PC client systems in the National Institute of Standards and Technology (NIST) specification for BIOS protection guidelines known as Special Publication 800-147. These improvements essentially 'lock the door', preventing unauthorized or unauthenticated BIOS and iDRAC firmware updates under any update scenarios, even if proper update procedures have not been followed for Dell digitally signed firmware update packages.

While this white paper focuses on the new PowerEdge 12th generation servers, the same improved security features are being made available for selected PowerEdge 11th generation servers and selected PowerEdge C servers from Dell.

Background

For an excellent background summary of BIOS principles and potential threats, please refer to section 2 of the National Institute of Standards and Technology (NIST) specification for BIOS Protection Guidelines known as Special Publication 800-147.

While this NIST document is client PC oriented, the BIOS concepts and security principles involved are easily extendable to servers. Dell has adapted and adopted these BIOS protection guidelines for our PowerEdge 12th generation servers, adding one more layer of security to our servers.

Key elements of enhancements to Dell firmware protection

Authenticated updates

Authentication ensures that BIOS and iDRAC update code comes from the authorized source, in this case from Dell. Update code for BIOS and iDRAC firmware are cryptographically signed. The server will do cryptographic verification of incoming update payload before allowing update operation to proceed.

Firmware Locking

To meet the requirements for a protected and signed BIOS update, the BIOS on the platform is locked and cannot be modified except by an authenticated update mechanism.

Non-bypassability

None of the other microcontrollers on the platform and none of the update mechanisms can circumvent the authenticated update mechanism for BIOS and/or iDRAC firmware updates.

No back flash to a non-compliant BIOS firmware

To the extent that early BIOS releases may exist that do not fully implement these BIOS and iDRAC firmware protection guidelines, BIOS and iDRAC firmware currently shipping on Dell PowerEdge 12th generation servers will not allow 'back flash' to a non-compliant firmware level.

BIOS versions incorporating enhancements to Dell firmware protection

The following table is a summary of the first BIOS version for each server which incorporates the enhancements to Dell firmware protection.

Server	BIOS Version
PowerEdge R820	1.0.0
PowerEdge R720	1.1.2
PowerEdge R720xd	1.1.2
PowerEdge R620	1.1.2
PowerEdge R520	1.0.0
PowerEdge R420	1.0.0
PowerEdge R320	1.0.0
PowerEdge T620	1.1.3
PowerEdge T420	1.0.1
PowerEdge T320	1.0.1
PowerEdge M820	1.0.0
PowerEdge M620	1.1.2
PowerEdge M520	1.0.0
PowerEdge M420	1.1.0

Summary

New BIOS and iDRAC firmware protection features introduced for our Dell PowerEdge 12th generation servers demonstrate Dell's leadership position in providing secure platforms for our PowerEdge server customers. These new features, combined with disciplined firmware update processes and procedures, provide Dell customers with a new elevated assurance level in securing server platforms for enterprise deployments.