DellEMC OpenManage Server Administrator – Deprecation of SHA1 Code Signing Certificates

The following sections provide a detailed description of this DellEMC OpenManage Server Administrator technical note.

Applies To

DellEMC OpenManage Server Administrator (OMSA) version 8.4 Microsoft Windows 2008 operating system variants (R2, 32–BIT, 64–BIT SP1, SP2)

Summary

This technical note provides information about the affected DellEMC OpenManage Server Administrator product version, upcoming product patch/release, and links to resources for additional information.

Microsoft has recently announced SHA1 deprecation policy and recommended upgrading to SHA2. The deprecation policy applies to certificates that include chain and intermediate, cryptographic applications use in SSL/TLS and code signing. Microsoft Security Advisory 2880823 announced that Microsoft would stop recognizing the validity of SHA1– based certificates after 2016.

The DellEMC OpenManage Server Administrator product team is helping users make the IT infrastructure more secure by proactively enabling, promoting and elevating strong cryptographic standards within SSL/TLS and code signing certificates. As part of this process, DellEMC OMSA product version 8.4 and later uses the SHA2 complaint certificates by default.

Systems running on the Windows Server 2008 OS may not be able to support SHA256 certificates because the operating system is not up-to-date with patching or upgrade. In this scenario, users may notice the following errors during certificate verification of DellEMC OMSA installer packages:

- Digital Signature Information — One of the countersignatures is not valid. The file may have been altered.
- Certificate Information — The timestamp signature and/or certificate could not be verified or is malformed.

NOTE: ***The DellEMC OMSA installation or functionality is not affected by certificate signature unrecognized by Windows Server 2008 environment.***

DellEMC recommends users to refer to the articles published on the Microsoft website and upgrade their system by installing the latest security patches.

Important Note

DellEMC recommends that the server platform is compliant with the new security standard and starts recognizing SHA256-signed certificates.

Additional Resources

For more details and the latest information on mitigations, see the following:

National Vulnerability Database: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-4004