Send documentation comments to mdsfeedback-doc@cisco.com

Security Advisory for OpenSSL Vulnerability in Cisco MDS 9000 Family Switches

CCO Date: May 14, 2007

Text Part Number: OL-5831-01

This document describes the OpenSSL vulnerability in the Cisco MDS 9000 Family switches and it provides recommendations to work around these issues.

Overview

The Cisco MDS 9000 Family of multilayer directors and fabric switches offer intelligent fabric-switching services that realize maximum performance while ensuring high reliability levels. They combine robust and flexible hardware architecture with multiple layers of network and storage management intelligence. This powerful combination enables highly available, scalable storage networks that provide advanced security and unified management features.

The Cisco MDS 9000 Family provides intelligent networking features such as multiprotocol and multitransport integration, virtual SANs (VSANs), advanced security, sophisticated debug analysis tools, and unified SAN management.

Background

Testing performed by the OpenSSL group using the Codenomicon TLS Test Tool uncovered a null-pointer assignment in the do_change_cipher_spec() function. A remote attacker could perform a carefully crafted Secure Sockets Layer/Transport Layer Security (SSL/TSL) protocol handshake against a server that uses an OpenSSL library and could cause OpenSSL to stop responding.

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Impact on the Cisco MDS 9000 Family

The HTTPS server uses OpenSSL for security services for Cisco MDS 9000 Family switches. Specifically, the HTTPS server provides authentication, data integrity, and confidentiality for the Storage Management Initiative specification (SMI-S). SMI-S enables storage area network (SAN) management clients to link to Common Information Model (CIM) servers and manages a large number of storage resources with a unified interface. The SMI-S interface is configured and managed through the MDS 9000 switches.

A user with malicious intent can create a denial-of-service (DoS) attack on the Cisco MDS 9000 Ethernet management port by sending synthetic messages. This vulnerability can be exploited to launch a DoS attack on the switch's control plane, hosted on the supervisor module. As a result of the DoS attack, the HTTPS server stops responding to SMI-S requests. It does not impact the existing data flows. The stateful process restart feature in Cisco MDS 9000 Family switches detects a HTTPS server failure and restarts the HTTPS server.

Note The OpenSSL vulnerability only exists on Cisco MDS 9000 switches running SAN-OS software Releases 1.3(1), 1.3(2a), and 1.3(3).

Solution and Recommendations

The OpenSSL vulnerability will be fixed in Cisco MDS SAN-OS Release 1.3(4).

We recommend the following workarounds for customers using Cisco MDS SAN-OS Releases: 1.3(1), 1.3(2a), and 1.3(3):

- Do not enable the SMI-S functionality if you do not need it to manage a Cisco MDS 9000 Family switch. By default, SMI-S is disabled in all switches in the Cisco MDS 9000 Family.

  To disable SMI-S, refer to the "Disabling CIM Support for the Cisco MDS 9000 Family" section in the *Cisco MDS 9000 Family SMI-S Programming Reference Guide*: http://www.cisco.com/en/US/products/ps6030/products_programming_reference_guide_book09186a0080698e30.html

- As a best practice, configure IP ACLs on Cisco MDS 9000 Family switches. This feature only allows trusted management entities to configure and manage Cisco MDS 9000 switches.

  To configure IP ACLs, refer to the "Configuring IP Services" section in the *Cisco MDS 9000 Family Configuration Guide* for SAN-OS Release 1.3x: http://www.cisco.com/en/US/products/ps5989/products_configuration_guide_book09186a008021a376.html

- As a best practice, deploy switches in the Cisco MDS 9000 Family in environments that are protected by firewall services. Configure the firewall to only allow trusted management entities.

Send documentation comments to mdsfeedback-doc@cisco.com