SR-680374472 SG500: Problemas de la vulnerabilidad con el SSL

Resumen

La exploración del Nessus encontró las vulnerabilidades en las habitaciones de la cifra soportadas.

Fecha identificada

Mayo 18, 2016

Fecha resuelta

De febrero el 17 de 2017

Productos afectados

SG500 Series	1.4.5.02

Descripción del problema

La exploración del Nessus muestra un algoritmo de troceo débil, una vulnerabilidad SSL. El servicio remoto utiliza una Cadena de certificados SSL que se ha firmado usando un algoritmo de troceo criptográficamente débil (e.g. MD2, MD4, MD5, o SHA1). Estos algoritmos de la firma se saben para ser vulnerables a los ataques de la colisión. Un atacante puede explotar esto para generar otro certificado con la misma firma digital, permitiendo que un atacante se disfrace como el servicio afectado.

Resolución

El problema debe ser reparado cuando usted actualiza a la versión 1.4.7.06 de la última versión de firmware.