SR-680374472 SG500 : Problèmes de vulnérabilité avec SSL

Résumé

Nessus scan a trouvé des vulnérabilités dans les suites de chiffrement prises en charge.

Date d'identification

18 mai 2016

Date de résolution

17 février 2017

Produits affectés

Série SG500	1.4.5.02

Description du problème

Nessus scan montre un algorithme de hachage faible, une vulnérabilité SSL. Le service distant utilise une chaîne de certificats SSL qui a été signée à l'aide d'un algorithme de hachage cryptographiquement faible (par exemple MD2, MD4, MD5 ou SHA1). Ces algorithmes de signature sont connus pour être vulnérables aux attaques de collision. Un pirate peut exploiter cela pour générer un autre certificat avec la même signature numérique, ce qui permet à un attaquant de se faire passer pour le service affecté.

Résolution

Le problème doit être résolu lors de la mise à niveau vers la dernière version du micrologiciel 1.4.7.06.