SR-680374472 SG500:SSLに関する脆弱性の問題

要約

Nessus scanでサポートされている暗号スイートの脆弱性が検出されました。

指定日

May 18, 2016

解決日

2017年2月17日

影響を受ける製品

SG500シリーズ	1.4.5.02

問題の説明

Nessusスキャンは、脆弱なハッシュアルゴリズムであるSSL脆弱性を示します。リモートサービスは、暗号化された脆弱なハッシュアルゴリズム (MD2、MD4、MD5、SHA1など) を使用して署名されたSSL証明書チェーンを使用します。 これらのシグニチャアルゴリズムは、コリジョン攻撃に対して脆弱であることが確認されています。攻撃者は、これを不正利用して同じデジタル署名を持つ別の証明書を生成し、攻撃者が該当サービスとしてマスカレードすることを可能にします。

解決方法

最新のファームウェアバージョン1.4.7.06にアップグレードする場合は、この問題を修正する必要があります。