SR-680374472 SG50: Schwachstellen bei SSL

Zusammenfassung

Nessus Scan hat Sicherheitslücken in unterstützten Verschlüsselungssuiten gefunden.

Identifiziertes Datum

18. Mai 2016

Auflösungsdatum

17. Februar 2017

Betroffene Produkte

SG500-Serie	1.4.5.02

Problembeschreibung

Nessus Scan zeigt einen schwachen Hash-Algorithmus, eine SSL-Schwachstelle. Der Remote-Dienst verwendet eine SSL-Zertifikatskette, die mit einem kryptografisch schwachen Hashing-Algorithmus signiert wurde (z. B. MD2, MD4, MD5 oder SHA1). Diese Signaturalgorithmen sind bekanntermaßen anfällig für Kollisionsangriffe. Ein Angreifer kann dies ausnutzen, um ein anderes Zertifikat mit derselben digitalen Signatur zu generieren, wodurch ein Angreifer sich als der betroffene Dienst tarnen kann.

Auflösung

Das Problem sollte behoben werden, wenn Sie auf die neueste Firmware-Version 1.4.7.06 aktualisieren.