SR-680374472 SG500:SSL的漏洞問題

摘要

Nessus掃描在支援的密碼套件中找到漏洞。

識別日期

2016年5月18日

解決日期

2017年2月17日

受影響的產品

SG500系列	1.4.5.02

問題描述

Nessus掃描顯示弱雜湊演算法，即SSL漏洞。遠端服務使用已使用加密弱雜湊演算法（例如MD2、MD4、MD5或SHA1）簽名的SSL證書鏈。 眾所周知，這些簽名演算法易受衝突攻擊。攻擊者可以利用此漏洞生成另一個具有相同數位簽章的證書，從而使攻擊者偽裝成受影響的服務。

解析

升級到最新韌體版本1.4.7.06時，問題應已解決。