ASR-680374472 SG500: Kwetsbaarheidskwesties met SSL

Samenvatting

Nessus scan ontdekte kwetsbaarheden in de door het algoritme ondersteunde series.

Datum geïdentificeerd

18 mei 2016

Datum opgelost

17 februari 2017

Producten getroffen

SG500 Series switch	1.4.5.02

Beschrijving van uitgifte

Nessus-scan toont een zwak hash-algoritme, een SSL-kwetsbaarheid. De afstandsbediening gebruikt een SSL-certificeringsketen die is ondertekend met behulp van een cryptografisch zwak hashingalgoritme (bv. MD2, MD4, MD5 of SHA1). Deze kenmerkende algoritmen zijn bekend om kwetsbaar te zijn voor botsingsaanvallen. Een aanvaller kan dit gebruiken om een ander certificaat te genereren met dezelfde digitale handtekening, wat een aanvaller in staat stelt zich voor te stellen als de getroffen dienst.

Resolutie

Probleem dient te worden opgelost bij het upgraden naar de nieuwste versie 1.4.7.06.