Beveiligingshulpmiddelen oplossen De paraplu-hoofdmap markeren CA

Inhoud

Inleiding

In dit document wordt beschreven waarom het digitale Umbrella Root CA-certificaat door beveiligingsauditingtools als een risico wordt gemarkeerd.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Umbrella Secure Web Gateway (SWG).

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Overzicht

Bepaalde beveiligingsauditingtools die worden gebruikt om Umbrella-infrastructuur te scannen, kunnen melden dat het digitale Cisco Umbrella Root CA-certificaat een 2048-bits RSA-sleutel heeft en een vervaldatum na 2030. Afhankelijk van de tool en het beveiligingsbeleid van de organisatie kan de sleutelgrootte en/of vervaldatum worden gemarkeerd als een risico dat moet worden verholpen. Bekijk de informatie in dit artikel om te bepalen of uw organisatie de aanbevelingen van de audittool moet accepteren.

Aanbevelingen van NIST

De aanbevelingen voor de lengte van digitale certificaatsleutels in de loop van de tijd (inclusief de datum van 2030 voor 2048-bits RSA-sleutels) werden uitgegeven door de Amerikaanse National Institutes of Standards (NIST). Het document met deze aanbevelingen is SP 800-57 Deel 1 Rev. 5: Aanbeveling voor sleutelbeheer.

"Tabel 4, Beveiligingssterkte tijdframes" (pagina 59) geeft aan dat een Beveiligingssterkte equivalent van 112 symmetrische sleutelbits geldig is na 2030 voor "Legacy gebruik" (RSA 2048-bit asymmetrische toetsen zijn gelijk aan ongeveer 116 bits symmetrische sleutelsterkte). Het gebruik van een bestaand root-certificaat zoals het Cisco Umbrella Root CA-certificaat valt in deze categorie, dus dit zou als compliant gebruik worden beschouwd. Het uitgeven van een certificaat met een 2048-bits sleutel na 2030 zou niet voldoen aan de aanbeveling.

Andere bekende publieke certificaatautoriteiten blijven rootcertificaten gebruiken met 2048-bits RSA-sleutels en vervaldatums na 2030. DigiCert-documentatie controleren: DigiCert Trusted Root Authority-certificaten voor voorbeelden, zoals het Global Root CA-certificaat en het Assured ID Root CA-certificaat, uitgegeven door DigiCert.

Ruim voor 2030 kan Cisco Umbrella een of meer nieuwe root-certificaten uitgeven met grotere sleutelgroottes die voldoen aan de NIST-aanbevelingen.

Aanvullende informatie

Organisaties zijn vrij om te beslissen of de NIST-aanbevelingen aan hun behoeften voldoen. Als u zich verder zorgen maakt over dit probleem, heeft Cisco een speciaal PKI-team dat toezicht houdt op het Trusted Root Store & PKI Compliance-programma van Cisco. Aanvullende informatie van het Cisco PKI-team (inclusief alle door Cisco uitgegeven openbare certificaten, certificaatbeleid en praktijkverklaringen en andere documentatie) is beschikbaar bij Cisco PKI: Policies, Certificates and Documents. Aanvullende vragen kunnen worden gemaild naar het PKI-team op ciscopki-public@external.cisco.com.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.