Lösen von Sicherheitstools, die die Umbrella Root CA kennzeichnen

Inhalt

Einleitung

In diesem Dokument wird erläutert, warum das digitale Zertifikat der Umbrella Root CA von Sicherheitsprüfungstools als Risiko gekennzeichnet wird.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Umbrella Secure Web Gateway (SWG).

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Überblick

Bestimmte Sicherheitsprüfungstools, die zum Scannen der Umbrella-Infrastruktur verwendet werden, können berichten, dass das digitale Zertifikat der Cisco Umbrella Root CA einen 2048-Bit-RSA-Schlüssel besitzt und nach 2030 abläuft. Je nach Tool und Sicherheitsrichtlinie kann die Schlüssellänge und/oder das Ablaufdatum als Risiko markiert werden, das ggf. behoben werden muss. Lesen Sie die Informationen in diesem Artikel durch, um festzustellen, ob Ihr Unternehmen die Empfehlungen des Auditing-Tools akzeptieren muss.

NIST-Empfehlungen

Die Empfehlungen für die Länge des Schlüssels für digitale Zertifikate (einschließlich des Datums 2030 für 2048-Bit-RSA-Schlüssel) wurden von den US National Institutes of Standards (NIST) herausgegeben. Das Dokument mit diesen Empfehlungen ist SP 800-57 Part 1 Rev. 5: Empfehlung für Schlüsselverwaltung.

"Table 4, Security strength time frames" (Seite 59) gibt an, dass ein Sicherheitsstärke-Äquivalent von 112 symmetrischen Schlüsselbits nach 2030 für "Legacy use" gültig ist (RSA 2048-Bit asymmetrische Schlüssel entsprechen etwa 116 Bit symmetrischer Schlüsselstärke). Die Verwendung eines vorhandenen Stammzertifikats, z. B. des Cisco Umbrella Root CA-Zertifikats, fällt in diese Kategorie, daher würde dies als konforme Verwendung betrachtet. Die Ausstellung eines Zertifikats mit einem 2048-Bit-Schlüssel nach 2030 würde der Empfehlung nicht entsprechen.

Andere bekannte öffentliche Zertifizierungsstellen verwenden weiterhin Stammzertifikate mit 2048-Bit-RSA-Schlüsseln und Ablaufdaten nach 2030. Lesen Sie die DigiCert-Dokumentation: Beispiele hierfür sind Zertifikate der vertrauenswürdigen Stammzertifizierungsstelle von DigiCert, z. B. das Zertifikat der globalen Stammzertifizierungsstelle und das Zertifikat der gesicherten ID-Stammzertifizierungsstelle, das von DigiCert ausgestellt wurde.

Bis weit vor 2030 kann Cisco Umbrella ein oder mehrere neue Stammzertifikate mit größeren Schlüsseln ausstellen, die den NIST-Empfehlungen entsprechen.

Zusätzliche Informationen

Die Organisationen können frei entscheiden, ob die NIST-Empfehlungen ihren Bedürfnissen entsprechen. Wenn Sie weitere Bedenken bezüglich dieses Problems haben, hat Cisco ein spezielles PKI-Team, das das Trusted Root Store- und PKI-Compliance-Programm von Cisco überwacht. Weitere Informationen vom Cisco PKI-Team (einschließlich aller von Cisco ausgestellten öffentlichen Zertifikate, Zertifikatrichtlinien und Verfahrensanweisungen sowie anderer Dokumentation) finden Sie unter Cisco PKI: Richtlinien, Zertifikate und Dokumente. Weitere Fragen können per E-Mail an das PKI-Team unter ciscopki-public@external.cisco.com gesendet werden.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.