Risoluzione degli strumenti di sicurezza che contrassegnano la CA radice Umbrella

Sommario

Introduzione

In questo documento viene descritto il motivo per cui il certificato digitale della CA radice Umbrella viene contrassegnato come rischio dagli strumenti di controllo della sicurezza.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni di questo documento si basano su Cisco Umbrella Secure Web Gateway (SWG).

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Panoramica

Alcuni strumenti di controllo della sicurezza utilizzati per eseguire la scansione dell'infrastruttura Umbrella possono segnalare che il certificato digitale Cisco Umbrella Root CA ha una chiave RSA a 2048 bit e una scadenza dopo il 2030. A seconda dello strumento e dei criteri di protezione dell'organizzazione, le dimensioni della chiave e/o la data di scadenza possono essere contrassegnate come un rischio che può richiedere l'intervento dell'utente. Esaminare le informazioni contenute in questo articolo per stabilire se l'organizzazione deve accettare i suggerimenti dello strumento di controllo.

Raccomandazioni NIST

Le raccomandazioni per la lunghezza della chiave del certificato digitale nel tempo (compresa la data del 2030 per le chiavi RSA a 2048 bit) sono state emesse dal National Institutes of Standards (NIST) degli Stati Uniti. Il documento contenente queste raccomandazioni è SP 800-57, parte 1, rev. 5: Suggerimento per la gestione delle chiavi.

La "Tabella 4, Security Strength Time Frame" (pagina 59) indica che un equivalente di Security Strength di 112 bit di chiave simmetrica è valido dopo il 2030 per "Uso legacy" (le chiavi asimmetriche RSA a 2048 bit equivalgono a circa 116 bit di forza della chiave simmetrica). L'utilizzo di un certificato radice esistente, ad esempio il certificato CA radice Cisco Umbrella, rientra in questa categoria, pertanto questo tipo di utilizzo viene considerato conforme. L'emissione di un certificato con una chiave a 2048 bit dopo il 2030 non sarebbe conforme alla raccomandazione.

Altre note autorità di certificazione pubblica continuano a utilizzare i certificati radice con chiavi RSA a 2048 bit e date di scadenza successive al 2030. Consultare la documentazione relativa a DigiCert: Certificati di autorità radice attendibili DigiCert per esempi, ad esempio il certificato CA radice globale e il certificato CA radice dell'ID garantito, rilasciati da DigiCert.

Ben prima del 2030, Cisco Umbrella può rilasciare uno o più nuovi certificati radice con chiavi di dimensioni maggiori conformi alle raccomandazioni NIST.

Ulteriori informazioni

Le organizzazioni sono libere di decidere se le raccomandazioni NIST soddisfano le loro esigenze. Per ulteriori dubbi su questo problema, Cisco dispone di un team PKI dedicato che supervisiona il programma di conformità Trusted Root Store & PKI di Cisco. Ulteriori informazioni del team Cisco PKI (tra cui tutti i certificati pubblici rilasciati da Cisco, i criteri e le istruzioni pratiche per i certificati e altra documentazione) sono disponibili all'indirizzo Cisco PKI: Criteri, certificati e documenti. Ulteriori domande possono essere inviate al team PKI all'indirizzo ciscopki-public@external.cisco.com.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).