

Comprendere l'effetto della migrazione della radice di GoDaddy sull'MRA di Expressway

Sommario

[Introduzione](#)

[Premesse](#)

[Specifiche del certificato](#)

[Radice precedente](#)

[CN: GoDaddy Root Certificate Authority - G2](#)

[Nuova radice](#)

[CN = GoDaddy TLS Root CA - R1](#)

[Nuovo livello intermedio](#)

[CN = GoDaddy TLS Intermediate CA DV - R1v1](#)

[Certificato con firma incrociata](#)

[CN = GoDaddy TLS Root CA - R1](#)

[Struttura certificati \(da nuova a vecchia\)](#)

[File importanti](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive l'effetto della migrazione del certificato radice GoDaddy da G2 a (R1 + R1V1).

Premesse

Transizione di GoDaddy dal criterio della vecchia radice (G2) alla nuova catena di certificati radice R1 in corso. I nuovi certificati devono includere solo l'utilizzo chiavi avanzato di autenticazione server.

Questa transizione ha effetto su expressway e altri prodotti periferici che hanno installato certificati GoDaddy.

La transizione delle radici avviene a causa di:

- Gli intermediari G2 di firma/rilascio non hanno alcun ECU elencato, il che rende tale gerarchia non conforme con il requisito del programma radice Chrome. Di conseguenza, il

rilascio da parte degli intermediari G2 interessati deve essere interrotto entro tale data.

- Nessun utilizzo chiavi avanzato indica che tutti gli scopi sono serviti da un certificato.

Specifiche del certificato

Radice precedente

CN: GoDaddy Root Certificate Authority - G2

Scadenza venerdì, gennaio 1, 2038 5:29:59

SN 00

Questa vecchia radice viene sostituita dalla nuova radice R1.

Nuova radice

CN = GoDaddy TLS Root CA - R1

Scadenza venerdì 24 agosto 24 2040 17.29.59

SN 00da62ff9e2619b1257a4809368ee8e3f7

La nuova radice R1 firma il nuovo intermedio come descritto nelle sezioni successive.

Nuovo livello intermedio

CN = GoDaddy TLS Intermediate CA DV - R1v1

Scadenza venerdì 24 agosto 24 2040 17.29.59

SN 008aaa80515c0bc688c7955d70f27758ac

Gli archivi dei trust del sistema operativo che hanno una vecchia radice G2 non considereranno

attendibile la nuova catena di certificati (R1 + R1V1) per questo scopo.

il nuovo certificato radice R1 considera attendibile il vecchio certificato radice G2.

Certificato con firma incrociata

CN = GoDaddy TLS Root CA - R1

Scadenza venerdì 1 gennaio 1 2038 5:29:59

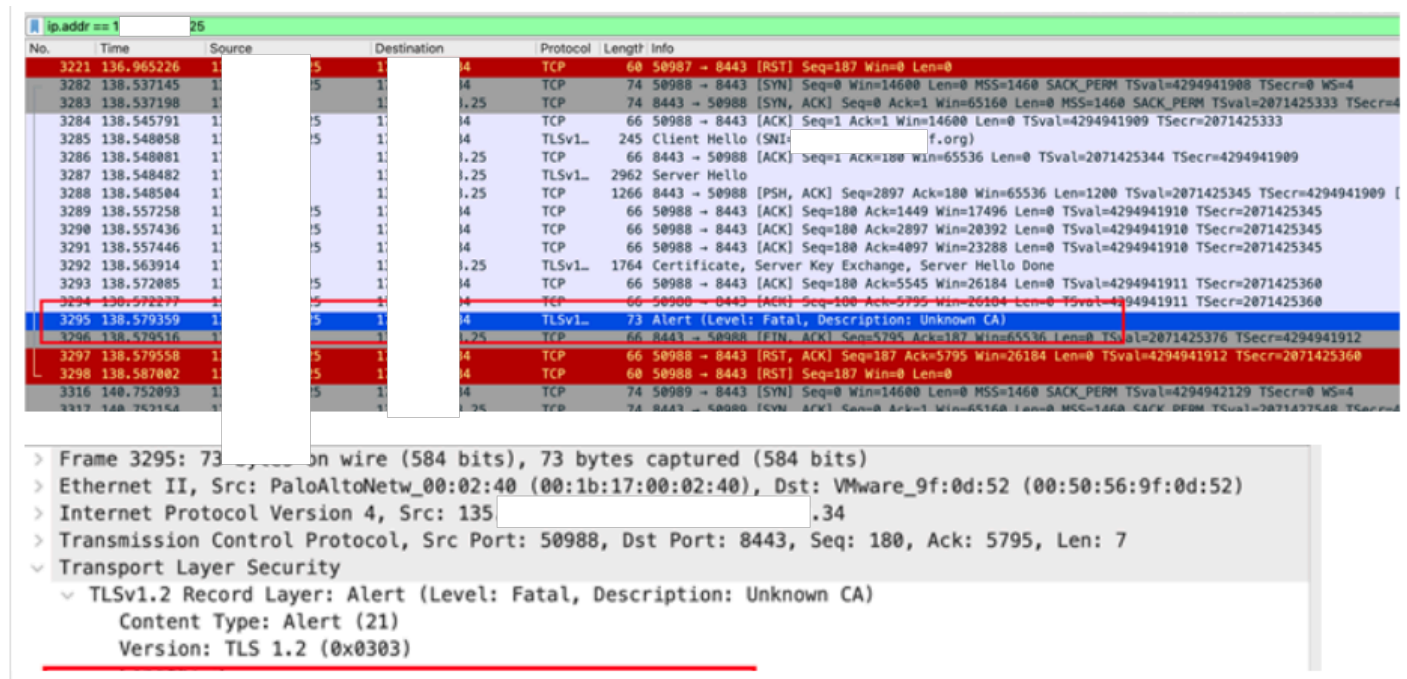
SN 0090de6c7fb3b50b3c0617724fc13402ad

Se non è stata installata la catena corretta o se è stata installata solo la nuova catena (R1 + R1v1) nell'archivio di Expressway Trust, la registrazione del telefono IP MRA verrà interrotta.

L'errore rilevato nella capsula EXPRESSWAY è un'autorità di certificazione sconosciuta proveniente da un telefono IP. Si presume che l'archivio attendibilità del telefono IP non contenga una CA.

88xx ip phone 135.x.x.25

172.x.x.34 Expressway



ip.addr == 172.25.0.34

No.	Time	Source	Destination	Protocol	Length	Info
3221	136.965226	172.25.0.34	172.25.0.34	TCP	60	50987 → 8443 [RST] Seq=187 Win=0 Len=0
3282	138.537145	172.25.0.34	172.25.0.34	TCP	74	50988 → 8443 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM TSval=4294941908 TSecr=0 WS=4
3283	138.537198	172.25.0.34	172.25.0.34	TCP	74	8443 → 50988 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=2071425333 TSecr=4
3284	138.545791	172.25.0.34	172.25.0.34	TCP	66	50988 → 8443 [ACK] Seq=1 Ack=1 Win=14600 Len=0 TSval=4294941909 TSecr=2071425333
3285	138.548058	172.25.0.34	172.25.0.34	TLSv1.2	245	Client Hello (SN=[redacted] f.org)
3286	138.548081	172.25.0.34	172.25.0.34	TCP	66	8443 → 50988 [ACK] Seq=1 Ack=180 Win=65536 Len=0 TSval=2071425344 TSecr=4294941909
3287	138.548482	172.25.0.34	172.25.0.34	TLSv1.2	2962	Server Hello
3288	138.548504	172.25.0.34	172.25.0.34	TCP	1266	8443 → 50988 [PSH, ACK] Seq=2897 Ack=180 Win=65536 Len=1200 TSval=2071425345 TSecr=4294941909
3289	138.557258	172.25.0.34	172.25.0.34	TCP	66	50988 → 8443 [ACK] Seq=180 Ack=1449 Win=17496 Len=0 TSval=4294941910 TSecr=2071425345
3290	138.557436	172.25.0.34	172.25.0.34	TCP	66	50988 → 8443 [ACK] Seq=180 Ack=2897 Win=20392 Len=0 TSval=4294941910 TSecr=2071425345
3291	138.557446	172.25.0.34	172.25.0.34	TCP	66	50988 → 8443 [ACK] Seq=180 Ack=4097 Win=23288 Len=0 TSval=4294941910 TSecr=2071425345
3292	138.563914	172.25.0.34	172.25.0.34	TLSv1.2	1764	Certificate, Server Key Exchange, Server Hello Done
3293	138.572085	172.25.0.34	172.25.0.34	TCP	66	50988 → 8443 [ACK] Seq=180 Ack=5545 Win=26184 Len=0 TSval=4294941911 TSecr=2071425360
3294	138.572277	172.25.0.34	172.25.0.34	TCP	66	50988 → 8443 [ACK] Seq=180 Ack=5795 Win=26184 Len=0 TSval=4294941911 TSecr=2071425360
3295	138.579359	172.25.0.34	172.25.0.34	TLSv1.2	73	Alert (Level: Fatal, Description: Unknown CA)
3296	138.579516	172.25.0.34	172.25.0.34	TCP	66	8443 → 50988 [FIN, ACK] Seq=5795 Ack=187 Win=65536 Len=0 TSval=2071425376 TSecr=4294941912
3297	138.579558	172.25.0.34	172.25.0.34	TCP	66	50988 → 8443 [RST, ACK] Seq=187 Ack=5795 Win=26184 Len=0 TSval=4294941912 TSecr=2071425360
3298	138.587082	172.25.0.34	172.25.0.34	TCP	60	50988 → 8443 [RST] Seq=187 Win=0 Len=0
3316	140.752093	172.25.0.34	172.25.0.34	TCP	74	50989 → 8443 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM TSval=4294942129 TSecr=0 WS=4

> Frame 3295: 73 bytes captured on wire (584 bits), 73 bytes captured (584 bits)

> Ethernet II, Src: PaloAltoNetw_00:02:40 (00:1b:17:00:02:40), Dst: VMware_9f:0d:52 (00:50:56:9f:0d:52)

> Internet Protocol Version 4, Src: 135.203.12.34

> Transmission Control Protocol, Src Port: 50988, Dst Port: 8443, Seq: 180, Ack: 5795, Len: 7

✓ Transport Layer Security

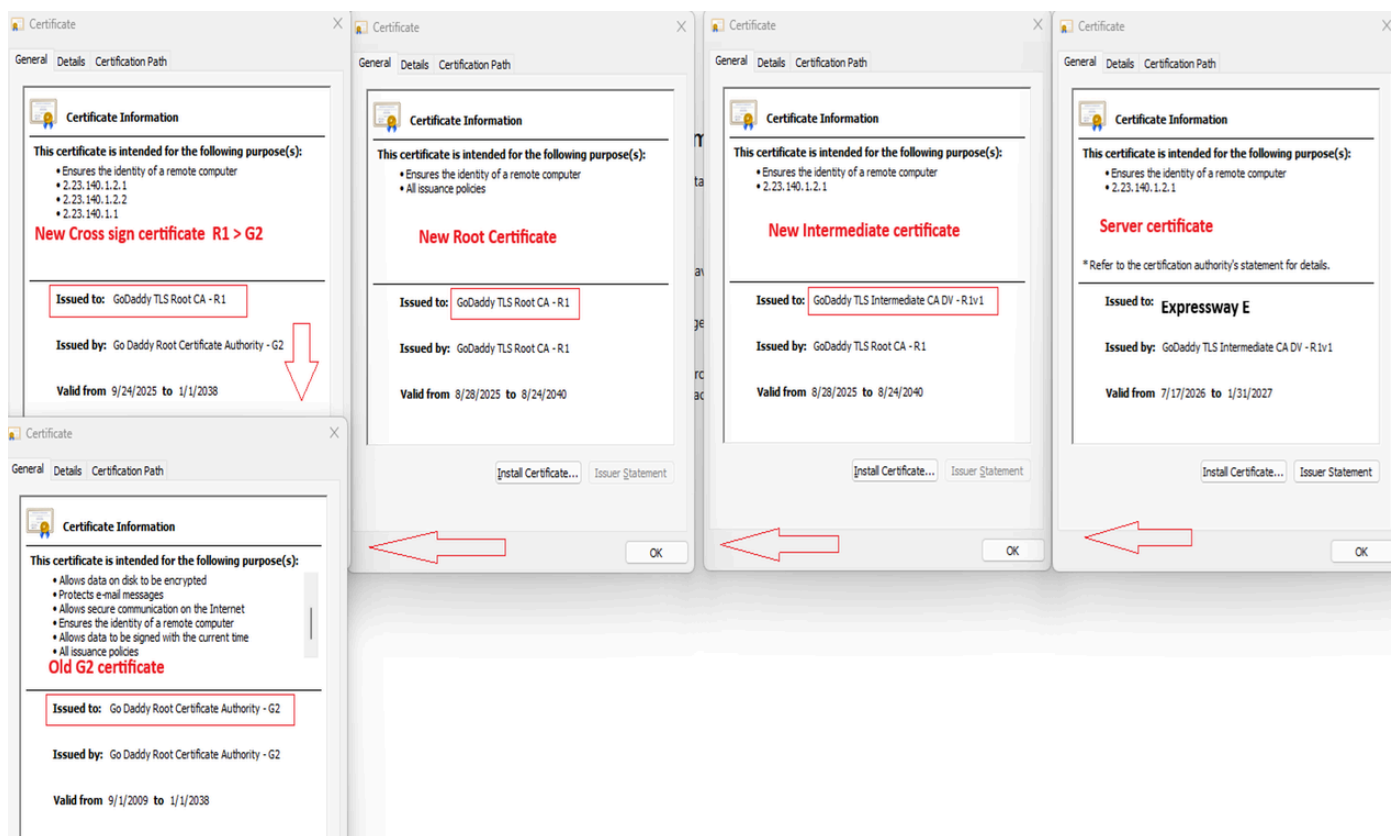
- TLv1.2 Record Layer: Alert (Level: Fatal, Description: Unknown CA)
Content Type: Alert (21)
Version: TLS 1.2 (0x0303)

In alcuni casi, l'archivio attendibilità di Expressway non accetta il certificato di firma incrociata perché il nuovo certificato radice e il nuovo certificato di firma incrociata hanno lo stesso nome CN, come in CN = GoDaddy TLS Root CA - R1.

In tal caso:

1. DELETE Nuovo certificato radice R1 SN 00da62ff9e2619b1257a4809368ee8e3f7.
2. Caricare il certificato di firma incrociata SN 0090de6c7fb3b50b3c0617724fc13402ad CN = GoDaddy TLS Root CA - R1.

Struttura certificati (da nuova a vecchia)



File importanti

Il certificato foglia viene rilasciato sotto la CA emittente R1 DV, ma i client lo convalidano costruendo una catena per GoDaddy Class 2 Root - G2 utilizzando il certificato incrociato R1 → G2 pubblicato. Gli artifact rilevanti nel repository sono il trust anchor G2 (gdroot-g2), il certificato incrociato (gd_tls_root-r1-cross-g2), l'intermedio di emissione R1 DV (gd_tls_issuer_dv-r1v1) e la radice della gerarchia nativa (gd_tls_root-r1) certs.godaddy.com. Questo approccio cross-sign consente ai browser di convalidare la catena oggi (ancorandola a G2), mentre il trust R1 si

propaga nel tempo.

Informazioni correlate

I dettagli sulla transizione dalla vecchia radice alla nuova radice sono documentati qui:

[Perché GoDaddy rimuove l'utilizzo chiavi avanzato ClientAuth e passa alla gerarchia radice R1 per il rilascio di DV TLS?](#)

Se si verifica questo problema, [qui](#) è il repository Godaddy per scaricare il certificato.

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).