

Comprender el efecto de la migración de la raíz de GoDaddy en Expressway MRA

Contenido

[Introducción](#)

[Antecedentes](#)

[Características del certificado](#)

[Raíz antigua](#)

[CN: Autoridad de certificados raíz de GoDaddy: G2](#)

[Nueva raíz](#)

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

[Nuevo intermedio](#)

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

[Certificado de firma cruzada](#)

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

[Árbol de certificados \(nuevo en antiguo\)](#)

[Archivos importantes](#)

[Información Relacionada](#)

Introducción

Este documento describe el efecto de migrar el certificado raíz de GoDaddy de G2 a (R1 + R1V1).

Antecedentes

GoDaddy está realizando la transición de la política de raíz antigua (G2) a la nueva cadena de certificados raíz R1. Los nuevos certificados deben incluir solamente la ECU de autenticación de servidor.

Esta transición afecta a autopistas y otros productos periféricos que tienen instalados certificados de GoDaddy.

La transición de raíces se realiza debido a:

- Los intermediarios de firmas/emisiones G2 no tienen ninguna ECU en la lista, lo que hace que esa jerarquía no cumpla con el requisito del programa raíz de Chrome. Por consiguiente, la emisión de los intermediarios del G2 afectados debe detenerse antes de

esa fecha.

- Sin ECU significa que todos los propósitos son servidos por certificado.

Características del certificado

Raíz antigua

CN: Autoridad de certificados raíz de GoDaddy: G2

Caducidad Viernes, 1 de enero de 2038 05:29:59

SN 00

Esta raíz antigua se reemplaza por la nueva raíz R1.

Nueva raíz

CN = CA raíz de TLS de GoDaddy - R1

Caducidad Viernes, 24 de agosto de 2040 5:29:59 p.m.

SN 00da62ff9e2619b1257a4809368ee8e3f7

La nueva raíz R1 firma el nuevo intermedio como se describe en las siguientes secciones.

Nuevo intermedio

CN = GoDaddy TLS intermedio CA DV - R1v1

Caducidad Viernes, 24 de agosto de 2040 5:29:59 p.m.

SN 008aaa80515c0bc688c7955d70f27758ac

Los almacenes de confianza del sistema operativo que tienen una antigua raíz G2 no confiarán en

la nueva cadena de certificados (R1 + R1V1) para este fin. GoDaddy ha creado una ruta de confianza de signo cruzado, donde

el nuevo certificado raíz R1 confía en el antiguo certificado raíz G2.

Certificado de firma cruzada

CN = CA raíz de TLS de GoDaddy - R1

Caducidad viernes, 1 de enero de 2038 05:29:59

SN 0090de6c7fb3b50b3c0617724fc13402ad

Si no tiene instalada la cadena correcta o solo tiene una cadena nueva (R1 + R1v1) instalada en el almacén de confianza de Expressway, el registro del teléfono IP de MRA se detiene.

El error observado en Expressway pcap es una CA desconocida que proviene de un teléfono IP. Puede suponer que falta una CA en el almacén de confianza del teléfono IP.

88xx ip phone 135.x.x.25

172.x.x.34 Expressway

The image shows a Wireshark packet capture of a TLS connection. The packet list on the left shows a sequence of packets from source 135.x.x.25 to destination 172.x.x.34. Packet 3295 is highlighted, showing a TLS alert (Level: Fatal, Description: Unknown CA). The packet details pane on the right shows the alert structure: Content Type: Alert (21), Version: TLS 1.2 (0x0303).

No.	Time	Source	Destination	Protocol	Length	Info
3221	136.965226	1	5	TCP	60	50987 → 8443 [RST] Seq=187 Win=0 Len=0
3282	138.537145	1	5	TCP	74	50988 → 8443 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM TSval=4294941908 TSecr=0 WS=4
3283	138.537198	1	5	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	1	5	TCP	66	50988 → 8443 [ACK] Seq=1 Ack=1 Win=14600 Len=0 TSval=4294941909 TSecr=2071425333
3285	138.548058	1	5	TLSv1	245	Client Hello (SN=[f.org])
3286	138.548081	1	5	TCP	66	8443 → 50988 [ACK] Seq=1 Ack=180 Win=65536 Len=0 TSval=2071425344 TSecr=4294941909
3287	138.548482	1	5	TLSv1	2962	Server Hello
3288	138.548504	1	5	TCP	1266	8443 → 50988 [PSH, ACK] Seq=2897 Ack=180 Win=65536 Len=1200 TSval=2071425345 TSecr=4294941909
3289	138.557258	1	5	TCP	66	50988 → 8443 [ACK] Seq=180 Ack=1449 Win=17496 Len=0 TSval=4294941910 TSecr=2071425345
3290	138.557436	1	5	TCP	66	50988 → 8443 [ACK] Seq=180 Ack=2897 Win=20392 Len=0 TSval=4294941910 TSecr=2071425345
3291	138.557446	1	5	TCP	66	50988 → 8443 [ACK] Seq=180 Ack=4097 Win=23288 Len=0 TSval=4294941910 TSecr=2071425345
3292	138.563914	1	5	TLSv1	1764	Certificate, Server Key Exchange, Server Hello Done
3293	138.572085	1	5	TCP	66	50988 → 8443 [ACK] Seq=180 Ack=5545 Win=26184 Len=0 TSval=4294941911 TSecr=2071425360
3294	138.572277	1	5	TCP	66	50988 → 8443 [ACK] Seq=180 Ack=5795 Win=26184 Len=0 TSval=4294941911 TSecr=2071425360
3295	138.579359	1	5	TLSv1	73	Alert (Level: Fatal, Description: Unknown CA)
3296	138.579516	1	5	TCP	66	8443 → 50988 [FIN, ACK] Seq=5795 Ack=187 Win=65536 Len=0 TSval=2071425376 TSecr=4294941912
3297	138.579558	1	5	TCP	66	50988 → 8443 [RST, ACK] Seq=187 Ack=5795 Win=26184 Len=0 TSval=4294941912 TSecr=2071425360
3298	138.587082	1	5	TCP	60	50988 → 8443 [RST] Seq=187 Win=0 Len=0
3316	140.752093	1	5	TCP	74	50989 → 8443 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM TSval=4294942129 TSecr=0 WS=4

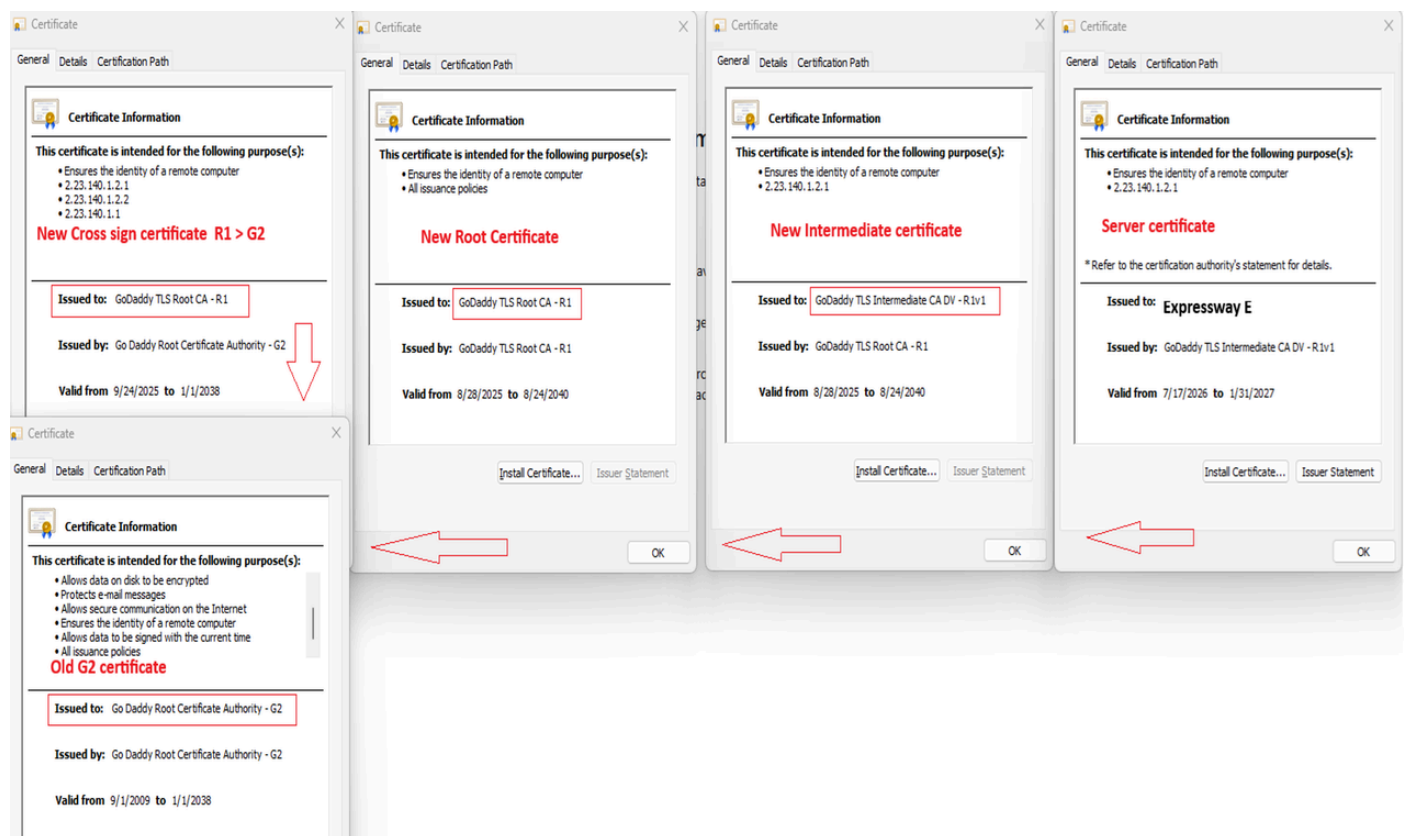
> Frame 3295: 73 bytes captured on wire (584 bits), 73 bytes captured (584 bits)
> Ethernet II, Src: PaloAltoNetw_00:02:40 (00:1b:17:00:02:40), Dst: VMware_9f:0d:52 (00:50:56:9f:0d:52)
> Internet Protocol Version 4, Src: 135.x.x.25, Dst: 172.x.x.34
> Transmission Control Protocol, Src Port: 50988, Dst Port: 8443, Seq: 180, Ack: 5795, Len: 7
✖ Transport Layer Security
 ✖ TLSv1.2 Record Layer: Alert (Level: Fatal, Description: Unknown CA)
 Content Type: Alert (21)
 Version: TLS 1.2 (0x0303)

También existe una situación en la que el almacén de confianza de Expressway no acepta el certificado de firma cruzada porque el nuevo certificado raíz y el certificado de firma cruzada tienen el mismo nombre CN, como en CN = GoDaddy TLS Root CA - R1.

En tal caso:

1. DELETE Nuevo certificado raíz R1 SN 00da62ff9e2619b1257a4809368ee8e3f7.
2. Cargue el certificado de firma cruzada SN 0090de6c7fb3b50b3c0617724fc13402ad CN = CA raíz de TLS de GoDaddy - R1.

Árbol de certificados (nuevo en antiguo)



Archivos importantes

El certificado de hoja se emite bajo la CA emisora de DV de R1, pero los clientes lo validan creando una cadena a GoDaddy Class 2 Root - G2 usando el certificado cruzado publicado de R1 → G2. Los artefactos relevantes en el repositorio son el anclaje de confianza G2 (gdroot-g2), el certificado cruzado (gd_tls_root-r1-cross-g2), el intermediario de emisión de DV R1 (gd_tls_issue_dv-r1v1) y la raíz de jerarquía nativa (gd_tls_root-r1) certs.godaddy.com. Este enfoque de firma cruzada permite a los navegadores validar la cadena hoy (anclando en G2),

mientras que la confianza de R1 se propaga con el tiempo.

Información Relacionada

Aquí se documentan los detalles sobre la transición de la raíz antigua a la nueva:

[¿Por qué GoDaddy elimina ClientAuth EKU y realiza la transición a la jerarquía raíz R1 para la emisión de DV TLS?](#)

En caso de que encuentre este problema, [aquí](#) está el repositorio de Godaddy para descargar el certificado.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).