El US-CERT emitió hoy una advertencia a los usuarios sobre una nueva vulnerabilidad de ejecución remota de código de 17 años, que afecta el software PPP daemon (pppd), que viene instalado en casi todos los sistemas operativos basados en Linux, y también alimenta el firmware de muchos otros dispositivos de red.

El software pppd afectado es una implementación del Protocolo punto a punto (PPP) que permite la comunicación y la transferencia de datos entre nodos, que se utiliza principalmente para establecer enlaces de Internet como los que se obtienen mediante módems de acceso telefónico, conexiones de banda ancha DSL y redes privadas virtuales.

Descubierto por la investigadora de seguridad de IOActive, Ilja Van Sorundel, el problema crítico es una vulnerabilidad de desbordamiento de búfer de pila que existe debido a un error lógico en el analizador de paquetes del Protocolo de Autenticación Extensible (EAP) del software pppd, una extensión que proporciona soporte para métodos de autenticación adicionales en conexiones PPP.

La vulnerabilidad, rastreada como CVE-2020-8597 con un puntaje CVSS de 9.8, puede ser explotada por atacantes no autenticados para ejecutar de forma remota código arbitrario en los sistemas afectamos y tomar el control total de estos.

Para lograr esto, lo que el hacker debe hacer es enviar un paquete EAP malformado no solicitado a un cliente ppp vulnerable o un servidor por medio de un enlace serie directo, ISDN, Ethernet, SSH, SOcket, CAT, PPTP, GPRS o redes ATM.

Además, debido a que pppd por lo general se ejecuta con privilegios altos y funciona en conjunto con los controladores del núcleo, la falla podría permitir a los atacantes ejecutar potencialmente código malicioso con el sistema o privilegios de nivel raíz.

> *«Esta vulnerabilidad se debe a un error al validar el tamaño de la entrada antes de copiar los datos suministrados en la memoria. Como la validación del tamaño de los datos es incorrecta, los datos arbitrarios se pueden copiar en la memoria y causar*

> *daños, lo que posiblemente conduzca a la ejecución de código no deseado»,* dice el aviso de seguridad.
>
> *«La vulnerabilidad está en la lógica del código de análisis de eap, específicamente en las funciones eap_request() y eap_response() en eap.c, que son llamadas por un controlador de entrada de red».*
>
> *«Es incorrecto suponer que pppd no es vulnerable si EAP no está habilitado o si EAP no ha sido negociado por un par remoto utilizando un secreto o frase de contraseña. Esto se debe al hecho de que un atacante autenticado aún puede enviar EAP no solicitado para activar el desbordamiento del búfer».*

Según la investigadora, las versiones 2.4.2 a 2.4.8 del Protocolo de punto a punto del daemon, todas las versiones lanzadas en los últimos 17 años son vulnerables a este problema.

Algunas de las distribuciones de Linux populares y ampliamente utilizadas, que se enlistan a continuación, ya se confirmaron como afectadas, y muchos otros proyectos probablemente estén afectados también.

- Debian
- Ubuntu
- SUSE Linux
- Fedora
- NetBSD
- RedHat Enterprise Linux

Además, la lista de otras aplicaciones y dispositivos vulnerables que envían el software ppd también es probablemente extensa, abriendo una gran superficie de ataque para los hackers.

Algunos de los productos afectados son:

- Cisco CallManager
- Productos TP-LINK
- SO Embebido OpenWRT
- Productos Synology