I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de Incidente: Falla de software / Vulnerabilidad (Buffer over-read – manejo incorrecto de memoria)
Nivel de riesgo: Alta

II. ALERTA

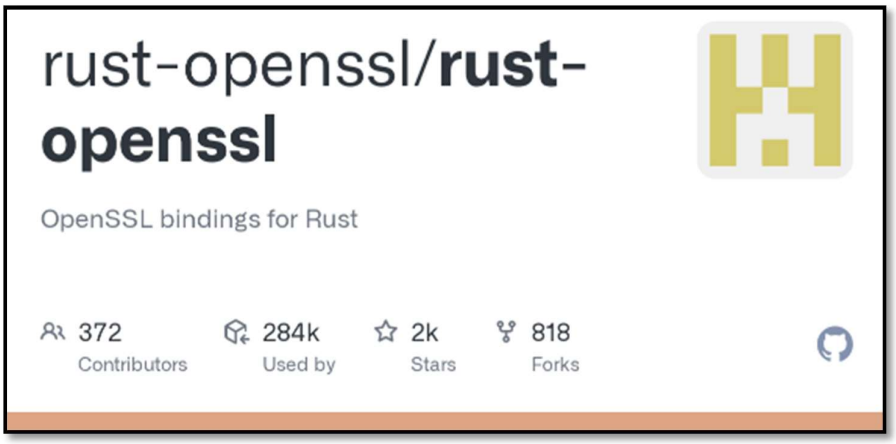

Figura 1.- Vulnerabilidad Crítica en rust-openssl (CVE-2026-41898) - Figura referencial

La librería rust-openssl encargada de proporcionar enlaces OpenSSL para el lenguaje de programación Rust, presenta una vulnerabilidad definida como CVE-2026-41898, la cual se trata de lectura fuera de límites (buffer over-read) y desbordamiento de memoria, lo que deriva en la exposición de información o comportamiento inesperado del sistema.

III. INTRODUCCIÓN

Rust-openSSL es la popular librería o crate como se denomina en Lenguaje Rust, la cual es la unidad fundamental de compilación y enlace del compilador (rustc), que proporciona enlaces (bindings) seguros para poder ser usados por la biblioteca de criptografía OpenSSL presenta 2 debilidades CWE-126 que es la lectura fuera de límites o *Buffer Over-read* y CWE-130 el manejo inadecuado de inconsistencia en parámetros de longitud, ambas debilidades derivan en que ocurre un manejo incorrecto de longitudes de funciones callbacks o que no se valida el tamaño del buffer y permite que los datos en memoria adyacente sean enviados a un peer remoto, con lo que se concreta exfiltración de información sensible.

IV. VECTOR DE ATAQUE

La vulnerabilidad CVE-2026-41898 tiene un vector de ataque tipo RED, CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H con nivel de severidad 9.8 CRITICA

Investigaciones indican que se origina en el manejo de funciones de callbacks dentro de la interfaz FFI (Foreign Function Interface) entre Rust y OpenSSL.

Específicamente, las funciones son:

- set_psk_client_callback
- set_psk_server_callback
- set_cookie_generate_cb
- set_stateless_cookie_generate_cb

Representando el siguiente problema:

- El valor retornado (usize) por una función definida por el usuario, es enviado directamente a OpenSSL sin validar si coincide con el tamaño real del buffer (&mut [u8]).

V. IMPACTO

- Explotación remota accesible a la red es posible sin necesidad de privilegios o interacción del usuario.
- La explotación exitosa podría dar lugar a la divulgación de información (alto impacto de confidencialidad), el compromiso de integridad de los datos y la interrupción de la disponibilidad.
- Los atacantes podrían crear entradas malintencionadas para desencadenar desbordamientos de buffer a través de las funciones de callbacks afectadas, lo que podría provocar fugas de información, denegación de servicio u otros efectos de corrupción de memoria.

VI. INDICADORES DE COMPROMISO

- Fallos inesperados en procesos TLS.
- Logs con errores en funciones de callbacks de OpenSSL.
- Comportamiento anómalo en manejo de buffers.
- Crashes o memory faults en aplicaciones Rust.
- Resultados inconsistentes en operaciones criptográficas

VII. RECOMENDACIONES:

- Actualizar inmediatamente a la versión 0.10.78 o superior.
- Validar correctamente tamaños de buffers en funciones de callbacks personalizados.
- Evitar confiar en valores retornados sin verificación.
- Revisar implementaciones que usen PSK o funciones de callbacks en TLS.
- Aplicar auditorías de seguridad en código que use FFI.
- Implementar pruebas de memoria (ASan, fuzzing) en entornos críticos.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

NIST (2026). CVE-2026-41898. https://nvd.nist.gov/vuln/detail/CVE-2026-41898

SECALERTS (2026). CVE-2026-41898 Vulnerability. https://secalerts.co/vulnerability/CVE-2026-41898

CVE DETAILS (2026). CVE-2026-41898. https://www.cvedetails.com/cve/CVE-2026-41898/

FEEDLY (2026). CVE-2026-41898. https://feedly.com/cve/CVE-2026-41898

SNYK (2026). SNYK-DEBIAN14-RUSTOPENSSL-16242470. https://security.snyk.io/vuln/SNYK-DEBIAN14-RUSTOPENSSL-16242470