Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

OPENSSL ADVIERTE DE LA EXISTENCIA DE UNA VULNERABILIDAD CRÍTICA.

31/Octubre/2022

Contenido

INTRODUCCIÓN

El proyecto OpenSSL ha anunciado una actualización con la que corregirán una vulnerabilidad de seguridad de gravedad crítica, de la que han preferido no compartir detalles por el momento.

OpenSSL es un proyecto de 'software' libre que ofrece un conjunto de herramientas y bibliotecas que aportan funciones criptográficas para la comunicación segura en Internet.

VULNERABILIDAD EN OPENSSL

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2022_10_31
Clasificación de alerta:	Vulnerabilidad
Tipo de Impacto:	Alto
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	10/31/2022
Es día cero (0 day):	Si

RESUMEN

A través de un comunicado, han anunciado una actualización de seguridad para su corrección, identificada con la versión 3.0.7 de OpenSSL, que se distribuirá el 1 de noviembre. Desde el proyecto OpenSSL han instado a las organizaciones para que estén atentos y parcheen sus sistemas.

En resumen: La actualización solo afectará a OpenSSL 3.0.x, no a 1.1.1. Ahora es el momento de averiguar dónde y cómo está utilizando OpenSSL 3.0.x. Para la mayoría de los sistemas, podrá utilizar la utilidad de línea de comandos de openssl:

% openssl version

La primera versión estable de OpenSSL 3.0, se lanzó en septiembre de 2021, hace aproximadamente un año. Es probable que cualquier sistema operativo anterior use OpenSSL 1.1.1, que no se ve afectado.

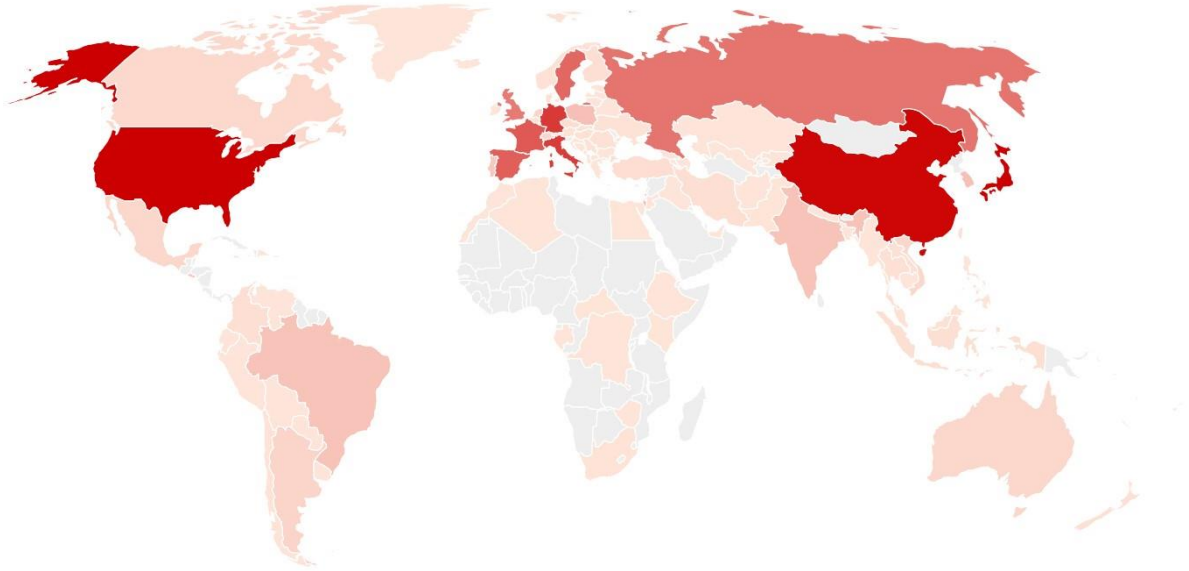
MacOS, de forma predeterminada, usa LibreSSL, no openssl, instalado. Pero openssl puede ser instalado más tarde por otro software como Homebrew y MacPorts.

En cuanto a las distros Linux, estas son las versiones de OpenSSL encontradas por defecto:

Linux Distro	OpenSSL Version
CentOS Linux release 7.9	1.0.2
CentOS 8	(1.1.1)
CentOS Stream 9	(3.0.1)
Debian 11 (bullseye)	(1.1.1)
Eneavour 2022.09.10	(1.1.1)
Fedora 34	(1.1.1)
Fedora 35	(1.1.1)
Fedora 36	(3.0.5)
Fedora Rawhide	(3.0.5)
Kali 2022.3	(3.0.5)
Linux Mint 21 Vanessa	(3.0.2)
Mageia 7	(1.1.1)
Mageia 8	(1.1.1)
Mageia Cauldron	(3.0.5)
OpenMandriva 4.3	(3.0.3)
OpenMandriva Cooker	(3.0.6)
OPNsense 22	1.1.1
OpenSuSE Leap 15.2	(1.1.1)
OpenSuSE Leap 15.3	(1.1.1)
OpenSuSE Leap 15.4	(1.1.1)
Proxmox 6	1.1.1
Redhat ES 9	3.0
Rocky Linux release 9.0 (Blue Onyx)	3.0.1
Slackware 14	1.0.1
Ubuntu 20.04	(1.1.1)
Ubuntu 22.04	(3.0.2)

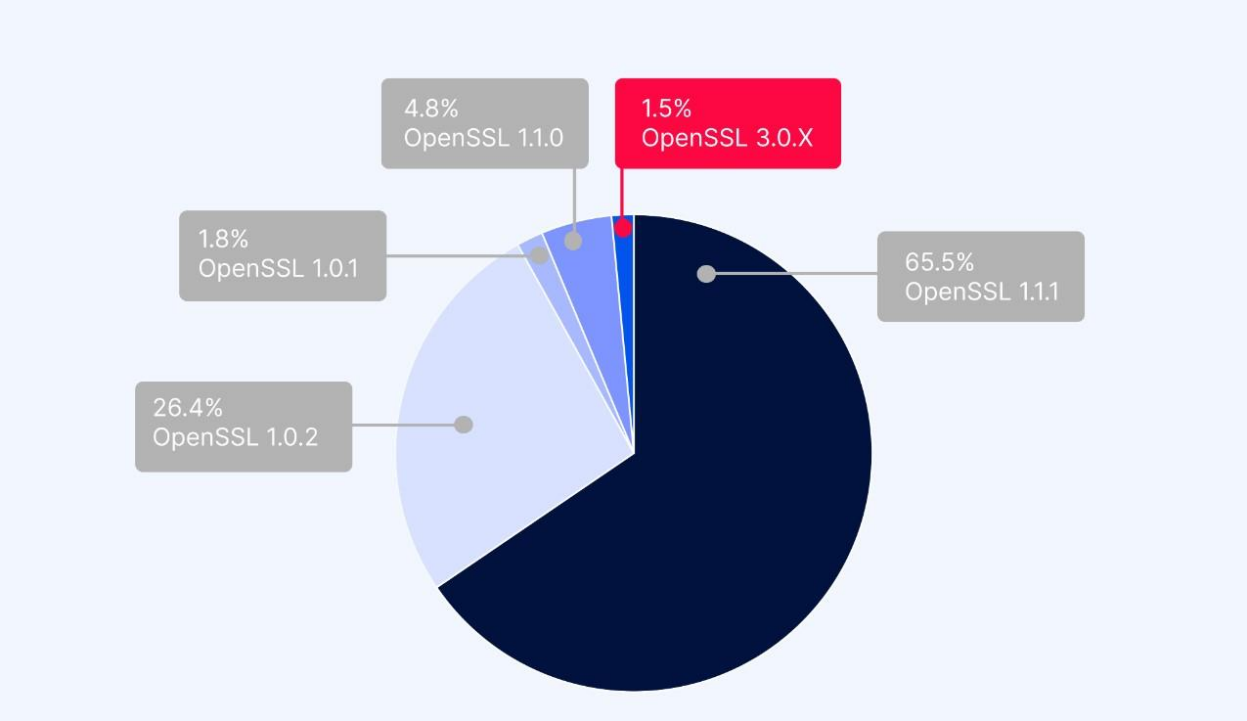
Vale la pena señalar que muchas imágenes populares de Docker Official usan Debian Bullseye (11) y Alpine, que todavía usan OpenSSL 1.x y no se ven afectadas. Las imágenes de contenedor oficiales de Docker para proyectos como nginx y httpd, populares para manejar el tráfico web, también usan Bullseye y Alpine y no se ven afectadas.

Finalmente, si sus propios desarrolladores usan C/C++, es posible que estén incorporando paquetes OpenSSL v3 en su código. Debe verificar este código para los paquetes OpenSSL relevantes.



Mapa de calor con host usando OpenSSL (Todas las versiones)

Para evaluar el impacto potencial de la vulnerabilidad, el equipo de Wiz Labs analizo cientos de entornos en la nube de todos los principales CSP (AWS, GCP, Azure, OCI y Alibaba Cloud) que contenían millones de cargas de trabajo. Descubriendo que más del 75 % de las organizaciones tienen al menos una instancia afectada en su entorno. Afortunadamente, solo el 1,5 % de las instancias de OpenSSL son versiones afectadas, mientras que el 98,5 % son versiones anteriores que no se ven afectadas.



Versiones más usadas de OpenSSL

RECOMENDACIONES

- Informe a los miembros del equipo sobre el anuncio de vulnerabilidad y el próximo lanzamiento de seguridad el próximo martes 1 de noviembre de 2022. Asegurarse de que su equipo esté al tanto del problema y el próximo lanzamiento es la mejor manera de prepararse.

- Identifique qué activos ejecutan versiones afectadas de OpenSSL.

- Evalúe sus aplicaciones e infraestructura para determinar si está utilizando o no OpenSSL 3.0 o superior en cualquier lugar.

- Prepárese para actualizar cualquier instalación OpenSSL vulnerable el martes 1 de noviembre de 2022.

Noticia Completa

https://devel.group/blog/openssl-advierte-de-la-existencia-de-una-vulnerabilidad-critica/

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757
El Salvador: +(503) 2249 4252
Honduras: +(504) 2283 5904
República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente