Nro. Alerta:	EC-2022-048	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	16-marzo-2022	**Vulnerabilidades que afectan a OpenSSL**	V 1.1

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de incidente: Sistema y/o Software Abierto
Nivel de riesgo: Alta

II. ALERTA

OpenSSL publicó una actualización de seguridad para contrarrestar un error de análisis del certificado que provocaría denegación de servicio.

Figura 1. Logotipo OpenSSL

III. INTRODUCCIÓN

OpenSSL es una herramienta de código abierto empleado para la autenticación WEB; a través, de los siguientes protocolos:

- SSL (Secure Socket Layer).
- TLS (Transport Layer Security).

A través de esos protocolos se encriptan los datos que se envían a otra computadora dentro de una red; de igual manera permite la desencriptación; evitando el acceso a la información por intrusos con la utilización de sniffer.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-048	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	16-marzo-2022	**Vulnerabilidades que afectan a OpenSSL**	V 1.1

En la siguiente tabla se describe el CVE asignado para esta vulnerabilidad

ÍTEM	CVE	DESCRIPCIÓN
1	CVE-2022-0778	Su explotación podría llevar a un ataque de denegación de servicio (DoS) contra un proceso que analice certificados provistos de forma externa. Es posible detonar un loop infinito creando un certificado que tenga parámetros inválidos

Tabla 1. Vulnerabilidad asociada a OpenSSL
Fuente: OpenSSL

IV. VECTOR DE ATAQUE: Red

La actual vulnerabilidad de OpenSSL consiste en un error en la función **BN_mod_sqrt(),** que si se explota por ejemplo a través de un certificado[1] con fines malintencionados para analizar; activará una función de bucle infinito y conduce a condiciones de denegación de servicio. El bucle infinito también puede ser alcanzado cuando se analizan claves privadas manipuladas, ya que pueden contener explícito parámetros de la curva elíptica.

En la siguiente tabla se mencionan las versiones afectadas.

ÍTEM	CVE	PRODUCTOS AFECTADOS
1	CVE-2022-0778	Este problema afecta a las versiones 1.0.2, 1.1.1 y 3.0 de OpenSSL

Tabla 2. CVE y productos afectados.
Fuente: Aviso de seguridad de OpenSSL

Las situaciones vulnerables incluyen:

- Clientes TLS que consumen certificados de servidor.
- Servidores TLS que consumen certificados de cliente.
- Proveedores de alojamiento que toman certificados o claves privadas de los clientes.
- Autoridades de certificación que analizan las solicitudes de certificación de los suscriptores.
- Cualquier otra cosa que analice los parámetros de la curva elíptica ASN.1

[1] El certificado debe contener claves públicas de curva elíptica en forma comprimida o parámetros de curva elíptica con un punto base codificada en forma comprimida para activar la falla.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-048	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	16-marzo-2022	**Vulnerabilidades que afectan a OpenSSL**	V 1.1

V. IMPACTO:

Las versiones de OpenSSL no brindan soporte para parámetros de curva elíptica personalizados; por esta razón, se ha calificado que la falla tiene un impacto de seguridad bajo.

A continuación, se menciona el impacto y la mitigación para cada una de las vulnerabilidades.

CVE	IMPACTO	MITIGACIÓN
CVE-2022-0778	Confidencialidad: Ninguna Integridad: Ninguna Disponibilidad: Elevado	• Los usuarios de OpenSSL 1.0.2 deben actualizar a 1.0.2zd (solo clientes de soporte premium) • Los usuarios de OpenSSL 1.1.1 deben actualizar a 1.1.1n • Los usuarios de OpenSSL 3.0 deben actualizar a 3.0.2

VI. RECOMENDACIONES:

El EcuCert recomienda a su comunidad objetivo:

- Instalar las respectivas actualizaciones entregadas por el proveedor.
- Implementar un plan de respuesta a emergencias de la Organización/Institución.

VII. REFERENCIAS:

Ecured. (s.f.). *Ecured*. Obtenido de Ecured: https://www.ecured.cu/OpenSSL

OpenSSL. (15 de 03 de 2022). *OpenSSL*. Obtenido de OpenSSL: https://www.openssl.org/news/secadv/20220315.txt

OpenSSL. (s.f.). *OpenSSL*. Obtenido de OpenSSL: https://www.openssl.org/

RedHat. (14 de 03 de 2022). *RedHat Customer Portal*. Obtenido de RedHat Customer Portal: https://access.redhat.com/security/cve/cve-2022-0778

Theastrologypage. (2022). *Theastrologypage*. Obtenido de Theastrologypage: https://es.theastrologypage.com/openssl

Toulas, B. (16 de 03 de 2022). *Bleepingcomputer*. Obtenido de Bleepingcomputer: https://www.bleepingcomputer.com/news/security/openssl-cert-parsing-bug-causes-infinite-denial-of-service-loop/