Alerta de seguridad cibernética	9VSA21-00414-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de marzo de 2021
Última revisión	29 de marzo de 2021

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información sobre vulnerabilidades dadas a conocer por OpenSSL Project.

Este informe incluye las medidas de mitigación, consistentes en instalar la última actualización de los productos afectados.

Vulnerabilidades

CVE-2021-3450
CVE-2021-3449

Impactos

CVE-2021-3450: Esta vulnerabilidad afecta a la verificación previa para confirmar que los certificados son válidos por la autoridad de certificación (CA). Podría permitir que un atacante pueda evitar por completo la verificación de un certificado, al no comprobar correctamente la validez de los mismos. Para verse afectado se debe tener activada la marca X509_V_FLAG_X509_STRICT, ya que no viene activada de manera predeterminada.

CVE-2021-3449: Esta vulnerabilidad existe debido a un error de desreferencia del puntero NULL al procesar las renegociaciones de TLSv1.2. Un atacante remoto puede enviar un mensaje ClientHello de renegociación creado con fines malintencionados. Esta vulnerabilidad permite a un atacante remoto realizar un ataque de denegación de servicio (DoS)

La explotación exitosa de estas vulnerabilidades podría autenticar un certificado de CA fraudulento o pueden realizar ataque de denegación de servicio (DoS), comprometiendo a los sistemas y a la infraestructura que la contiene.

Productos Afectados

CVE-2021-3450
OpenSSL versiones 1.1.1h, 1.1.1i, 1.1.1j

CVE-2021-3449
OpenSSL versiones 1.1.1x anteriores a 1.1.1k

OpenSSL 1.0.2 y 1.1.0 están fuera de soporte y ya no reciben actualizaciones. Se recomienda a los usuarios de estas versiones actualizar a OpenSSL 1.1.1k.

Mitigación

Instalar las respectivas actualizaciones desde el sitio web del proveedor.

OpenSSL es utilizado en ampliamente en el mercado, por ese motivo se adjuntan algunas referencias relativas a distintos productos que utilizan OpenSSL, y sus respectivas medidas de mitigación.

Cisco: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-openssl-2021-GHY28dJd

Netapp: https://security.netapp.com/advisory/ntap-20210326-0006/

FredBSD: https://www.freebsd.org/security/advisories/FreeBSD-SA-21:07.openssl.asc

Redhat: https://access.redhat.com/security/cve/CVE-2021-3450
https://access.redhat.com/security/cve/CVE-2021-3449

Ubuntu: https://ubuntu.com/security/cve-2021-3449

Enlaces

https://www.openssl.org/news/vulnerabilities.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3450
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3449

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.03.29 22:43:20 -03'00'