Alerta de seguridad cibernética	9VSA20-00213-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de mayo de 2020
Última revisión	15 de mayo de 2020

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 la información obtenida de FreeBSD referente a tres vulnerabilidades que afectan al Sistema Operativo. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidades

CVE-2020-15878
CVE-2020-15879
CVE-2020-15880

CVE-2020-15878

Debido a que la capa “SCTP” no valida correctamente cuando una aplicación intenta actualizar una llave compartida, un usuario local podría gatillar un error de uso de memoria luego de ser liberada con secuencias especificas de actualización de la llave compartida y cerrando la asociación “SCTP”, comprometiendo completamente al sistema afectado.

Producto Afectado
FreeBSD versión 11.3.

Mitigación
Aplicar los parches publicados por los desarrolladores.

Enlaces
https://www.freebsd.org/security/advisories/FreeBSD-SA-20:14.sctp.asc
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15878

CVE-2020-15879

Debido a una condición de carrera en el modulo “cryptodev”, un usuario local podría ejecutar una aplicación especialmente diseñada, para gatillar un error en memoria y sobrescribir de forma arbitraria la memoria del kernel, comprometiendo al sistema afectado.

Producto Afectado
Todas las versiones de FreeBSD.

Mitigación
Aplicar los parches publicados por los desarrolladores.

Enlaces
https://www.freebsd.org/security/advisories/FreeBSD-SA-20:15.cryptodev.asc
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15879

CVE-2020-15880

Debido a la insuficiente validación de datos ingresados por el usuario, al ingresar el largo de la llave MAC en el módulo "cryptodev". Es posible entregar una llave muy larga para gatillar el error en memoria y comprometer completamente al sistema afectado.

Producto Afectado

FreeBSD versión 12.1.

Mitigación

Aplicar los parches publicados por los desarrolladores.

Enlaces

https://www.freebsd.org/security/advisories/FreeBSD-SA-20:16.cryptodev.asc
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15880