Alerta de seguridad informática	9VSA-00083-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de octubre de 2019
Última revisión	08 de octubre de 2019

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 entregada por diferentes fuentes, referente a una vulnerabilidad en la biblioteca de compresión 'libarchive', utilizada en múltiples distribuciones de Linux, FreeBSD y NetBSD, la cual permite generar ataques de tipo ejecución de código remoto. También se comparte su respectiva forma de mitigarla.

Vulnerabilidad

CVE-2019-18408

Impacto

La biblioteca 'libarchive', ocupada para leer y crear archivos comprimidos entre otras funcionalidades, al no validar correctamente los datos procesados, permite, utilizando un archivo especialmente diseñado, acceder a la memoria luego de su uso, lo cual se podría aprovechar para generar ataques de ejecución de código remoto, por ende, comprometer al sistema en múltiples maneras.

Productos Afectados

Archivo 'libarchive' versiones anteriores a la 3.4.0 en los sistemas operativos Debian, Ubuntu, Gentoo, Arch Linux, FreeBSD y NetBSD.

Mitigación

Actualizar a la versión 3.4.0 de 'libarchive', a través de las actualizaciones indicadas por los diferentes fabricantes.

Enlace

- https://nvd.nist.gov/vuln/detail/CVE-2019-18408
- https://security-tracker.debian.org/tracker/source-package/libarchive
- https://usn.ubuntu.com/4169-1/
- https://bugs.gentoo.org/show_bug.cgi?id=CVE-2019-18408

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.11.08 12:13:23 -03'00'