Alerta de seguridad informática	**9VSA-00026-001**
Clase de alerta	**Vulnerabilidad**
Tipo de incidente	**Sistema y/o Software Abierto**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**30 de Julio de 2019**
Última revisión	**30 de Julio 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 Ubuntu acerca de vulnerabilidades que afectan a OpenLDAP.

Vulnerabilidad

- CVE-2019-13057
- CVE-2019-13565

Impacto

CVE-2019-13057
Se descubrió que OpenLDAP manejaba incorrectamente la delegación de rootDN. Un administrador de la base de datos podría usar este problema para solicitar autorización como identidad de otra base de datos, en contra de lo esperado.

CVE-2019-13565
Se descubrió que OpenLDAP manejaba incorrectamente la autenticación SASL y el cifrado de sesión. Después de completar un primer enlace SASL, fue posible obtener acceso mediante enlaces simples, en contra de lo esperado.

Productos Afectados

OpenLDAP versiones anteriores a 2.4.48

Mitigación

El problema puede ser corregido actualizando a la versión 2.4.48

Enlace

https://usn.ubuntu.com/4078-1/
https://www.openldap.org/lists/openldap-announce/201907/msg00001.html
http://www.openldap.org/software/download/

CSIRT
Gobierno de
Chile

Firmado digitalmente
por CSIRT Gobierno
de Chile
Fecha: 2019.07.30
19:14:07 -04'00'