Alerta de seguridad informática	9VSA20-00127-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Enero de 2020
Última revisión	23 de Enero 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 información obtenida de Samba, referente a vulnerabilidades que afectan a su herramienta de servicios de archivos e impresiones para Microsoft, las cuales de ser explotadas permitirían a un atacante remoto (vía LAN) obtener recursos sensibles y realizar ataques de denegación de servicios, Este informe incluye la respectiva mitigación.

Vulnerabilidades

CVE-2019-14902

CVE-2019-14907

CVE-2019-19344

Impacto

CVE-2019-14902

Un atacante podría evitar las verificaciones de seguridad obteniendo acceso a recursos sensibles debido a la ausencia de una replicación de sincronización completa que no permite que los cambios de ACL se efectuaran en todos los controladores de un dominio.

CVE-2019-14907

Un atacante podría realizar ataques de denegación de servicio debido al incorrecto procesamiento de ciertos datos controlados por el usuario, si es que el registro está habilitado en el nivel 3 o superior, dando paso a la posibilidad de enviar datos especialmente diseñados a Samba DC y finalizar el trabajo del servidor Samba RPC.

CVE-2019-19344

Esta vulnerabilidad permitiría a un atacante obtener acceso a información sensible debido a un error en memoria durante la eliminación de zonas en el DNS. Bajo condiciones especiales, se le podría enviar consultas al DNS y obtener partes de la memoria que fueron escritas en la base de datos durante el proceso de eliminación de zonas.

Productos Afectados

Samba desde la versión 4.0 hasta la 4.11.4.
Para el CVE-2019-19344 desde la versión 4.9 hasta la 4.11.4.

Mitigación

Para 4.x hasta 4.9.x, actualizar a la versión 4.9.18.
Para 4.10.x, actualizar a la versión 4.10.12.
Para 4.11.x, actualizar a la versión 4.11.5.

Enlaces

https://www.samba.org/samba/security/CVE-2019-14902.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2019-14902
https://www.samba.org/samba/security/CVE-2019-14907.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2019-14907
https://www.samba.org/samba/security/CVE-2019-19344.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2019-19344