Alerta de seguridad cibernética	9VSA20-00291-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de agosto de 2020
Última revisión	24 de agosto 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 PostgreSQL referente a dos vulnerabilidades que afectan gravemente a la integridad y confidencialidad de la base de datos. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidades

CVE-2020-14349
CVE-2020-14350

CVE-2020-14349

La configuración “search_path” determina los esquemas buscados para tablas, funciones, operadores, etc. El arreglo CVE-2018-1058 causaba que la mayoría de las aplicaciones sanitizaran “search_path”, pero la replicación lógica dejaba al parámetro sin cambios. Usuarios del sistema de replicación publisher y subscritos a la base de datos pueden crear objetos en el esquema público y aprovecharlos para ejecutar sentencias SQL utilizando el usuario de la replicación, en su mayoría, el superuser.

Productos Afectados
PostgreSQL desde la versión 10 hasta la 12.

Mitigaciones
Actualizar a la versión 10.14, 11.9 o 12.4.

Enlaces
https://www.postgresql.org/about/news/2060/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14349

CVE-2020-14350

Cuando un superuser ejecuta ciertas sentencias “CREATE EXTENSION”, los usuarios pueden ejecutar las funciones SQL arbitrarias bajo la identidad de ese usuario. El atacante debe tener permiso para crear objetos en el esquema de la nueva extensión o un esquema de una extensión de requisito previo.

Productos Afectados
PostgreSQL desde la versión 9.5 hasta la 12.

Mitigaciones
Actualizar a la versión 9.5.23, 9.6.19, 10.14, 11.9 o 12.4.

Enlaces
https://www.postgresql.org/about/news/2060/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14350