Alerta de seguridad cibernética	9VSA21-00365-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de enero de 2021
Última revisión	16 de enero de 2021

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 Red Hat, sobre cuatro vulnerabilidades que afectan a algunos sus productos.

Este informe incluye las medidas de mitigación, consistentes en instalar la última actualización de los productos afectados.

Vulnerabilidades

CVE-2020-24553
CVE-2020-28362
CVE-2020-28366
CVE-2020-28367

Impacto

Dos vulnerabilidades son de riesgo alto: CVE-2020-28366 y CVE-2020-28367 permiten a un atacante remoto ejecutar código arbitrario en el sistema objetivo. La vulnerabilidad existe debido a una validación inapropiada de la información ingresada al momento de compilar, cuando el código cgo está en uso. Un atacante remoto puede engañar a la víctima para que compile una aplicación especialmente diseñada y ejecutar código arbitrario en el sistema objetivo.

Productos afectados

Paquetes Red Hat OpenShift Serverless 0.2.3-1.el8 a 0.12.0-1.el8.

Mitigación

Instalar las actualizaciones desde el sitio del proveedor.

Enlaces

https://access.redhat.com/errata/RHSA-2021:0145

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28353

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28362

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28366

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28367