Alerta de seguridad cibernética	9VSA21-00442-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de mayo de 2021
Última revisión	10 de mayo 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 de Gobierno, comparte vulnerabilidades que afectan a distintos productos de Red Hat.

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

Vulnerabilidades

CVE-2020-28469
CVE-2021-23358
CVE-2021-28092
CVE-2021-29418
CVE-2021-28918
CVE-2021-20305
CVE-2020-25649
CVE-2021-2163
CVE-2021-3347
CVE-2021-3447
CVE-2021-20305
CVE-2021-27363
CVE-2021-27364
CVE-2021-27365

Impactos

Las siguientes vulnerabilidades fueron calificadas de riesgo alto:

CVE-2021-20305: Esta vulnerabilidad en Red Hat OpenShift Container Platform permite a un atacante remoto no autenticado ejecutar código arbitrario, debido a un error en Nettle (versiones anteriores a la 3.7.2) que permite a un atacante forzar una firma inválida. Esta vulnerabilidad amenaza la confidencialidad, integrad y disponibilidad del sistema.

CVE-2021-3447: Esta vulnerabilidad en Red Hat OpenShift Container Platform existe debido a la forma en que el software guarda información en los logs. Un usuario local puede leer los archivos log y acceder a datos sensibles.

CVE-2021-23358: Esta vulnerabilidad en Red Hat Advanced Cluster Management for Kubernetes permite a un atacante remoto ejecutar código arbitrario en el sistema objetivo. Ocurre debido a una validación inapropiada del input del usuario.

CVE-2021-20305: Esta vulnerabilidad en Red Hat Advanced Cluster Management for Kubernetes permite a un atacante remoto no autenticado ejecutar código arbitrario. debido a un error en Nettle (versiones anteriores a la 3.7.2) que permite a un atacante forzar una firma inválida. Esta vulnerabilidad amenaza la confidencialidad, integrad y disponibilidad del sistema.

Productos Afectados

Red Hat OpenShift Container Platform 4.6.0 a 4.6.26.
Red Hat Advanced Cluster Management for Kubernetes 2.2.0 a 2.2.2

Mitigación

Instalar las respectivas actualizaciones desde el sitio web del proveedor.

Enlaces

https://access.redhat.com/errata/RHSA-2021:1499
https://access.redhat.com/errata/RHSA-2021:1429
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28469
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23358
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28092
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29418
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28918
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-20305
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25649
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-2163
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3347
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3447
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-20305
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27363
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27364
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27365

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.05.10 12:59:10 -04'00'