Alerta de seguridad cibernética	9VSA21-00510-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de octubre de 2021
Última revisión	22 de octubre 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 del Gobierno de Chile, CSIRT de Gobierno, comparte información sobre vulnerabilidades recientemente publicadas por Red Hat.

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

Vulnerabilidades

CVE-2016-4658
CVE-2016-4658
CVE-2020-25648
CVE-2021-21670
CVE-2021-21671
CVE-2021-22543
CVE-2021-22922
CVE-2021-22923
CVE-2021-22924
CVE-2021-23017
CVE-2021-23840
CVE-2021-23841
CVE-2021-25741
CVE-2021-28169
CVE-2021-32626
CVE-2021-32627
CVE-2021-32628
CVE-2021-32672
CVE-2021-32675
CVE-2021-32687
CVE-2021-32690
CVE-2021-33196
CVE-2021-34428
CVE-2021-35550
CVE-2021-35556
CVE-2021-35559
CVE-2021-35561
CVE-2021-35564
CVE-2021-35565
CVE-2021-35567
CVE-2021-35578
CVE-2021-35586
CVE-2021-35588
CVE-2021-35603
CVE-2021-36222
CVE-2021-3653
CVE-2021-3656
CVE-2021-36980
CVE-2021-37576
CVE-2021-37750
CVE-2021-41099

Impactos

Vulnerabilidades de riesgo alto:

CVE-2021-36980: Esta vulnerabilidad existe debido a un error de uso de memoria luego de ser liberada en decode_NXAST_RAW_ENCAP durante la decodificación de una acción RAW_ENCAP. Un atacante remoto puede enviar una solicitud especialmente diseñada al sistema, detonar un error de uso de memoria después de ser liberada y ejecutar código arbitrario, pudiendo gracias a ello comprometer un sistema vulnerable.

CVE-2021-41099: Esta vulnerabilidad existe debido a un error de desborde de enteros al manipular input no confiable, y permite a un atacante remoto ejecutar código arbitrario en el sistema objetivo.

CVE-2016-4658: Esta vulnerabilidad existe debido a un error de memoria luego de ser liberada, lo que permite a un atacante remoto usar un documento XML especialmente creado para generar el error y ejecutar código arbitrario en el sistema.

CVE-2021-32628: Esta vulnerabilidad existe debido a un error de desborde de enteros. Su explotación exitosa puede permitir el compromiso total de un sistema vulnerable.

CVE-2021-32627: Esta vulnerabilidad existe debido a un error de desborde de enteros. Su explotación exitosa puede permitir el compromiso total de un sistema vulnerable.

CVE-2021-23017: Esta vulnerabilidad existe debido a un error al procesar solicitudes DNS, el que puede ser detonado por un atacante remoto. Su explotación exitosa puede permitir el compromiso total de un sistema vulnerable.

Productos Afectados

java-1.8.0-openjdk (Red Hat package): before 1.8.0.312 b07-1.el8_1
java-1.8.0-openjdk (Red Hat package): before 1.8.0.312 b07-1.el8_2
java-1.8.0-openjdk (Red Hat package): before 1.8.0.312 b07-1.el8_4
java-11-openjdk (Red Hat package): 11.0.11.0.9-0.el8_2, 11.0.12.0.7-0.el8_2
java-11-openjdk (Red Hat package): 11.0.11.0.9-1.el7_9, 11.0.12.0.7-0.el7_9
java-11-openjdk (Red Hat package): 11.0.12.0.7-0.el8_4
java-11-openjdk (Red Hat package): 11.0.6.10-0.el8_1, 11.0.7.10-1.el8_1, 11.0.11.0.9-0.el8_1, 11.0.12.0.7-0.el8_1
openvswitch2.11 (Red Hat package): 2.11.3-77.el7fdp, 2.11.3-86.el7fdp
Red Hat Advanced Cluster Management for Kubernetes 2.1
Red Hat Advanced Cluster Management for Kubernetes: 2.3.0, 2.3.1, 2.3.2
Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support: 8.4
Red Hat CodeReady Linux Builder for ARM 64: 8.0
Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support: 8.4
Red Hat CodeReady Linux Builder for IBM z Systems: 8.0
Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support: 8.4
Red Hat CodeReady Linux Builder for Power, little endian: 8.0

Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support: 8.4
Red Hat CodeReady Linux Builder for x86_64: 8.0
Red Hat Enterprise Linux Desktop: 7
Red Hat Enterprise Linux for ARM 64 - Extended Update Support: 8.1
Red Hat Enterprise Linux for ARM 64 - Extended Update Support: 8.4
Red Hat Enterprise Linux for ARM 64: 8
Red Hat Enterprise Linux for IBM z Systems - Extended Update Support: 8.1
Red Hat Enterprise Linux for IBM z Systems - Extended Update Support: 8.4
Red Hat Enterprise Linux for IBM z Systems: 7
Red Hat Enterprise Linux for IBM z Systems: 8
Red Hat Enterprise Linux for Power, big endian: 7
Red Hat Enterprise Linux for Power, little endian - Extended Update Support: 8.1
Red Hat Enterprise Linux for Power, little endian - Extended Update Support: 8.4
Red Hat Enterprise Linux for Power, little endian: 7
Red Hat Enterprise Linux for Power, little endian: 8
Red Hat Enterprise Linux for Scientific Computing: 7
Red Hat Enterprise Linux for x86_64 - Extended Update Support: 8.1
Red Hat Enterprise Linux for x86_64 - Extended Update Support: 8.4
Red Hat Enterprise Linux for x86_64: 8.0
Red Hat Enterprise Linux Server - AUS: 8.4
Red Hat Enterprise Linux Server - TUS: 8.2
Red Hat Enterprise Linux Server - TUS: 8.4
Red Hat Enterprise Linux Server - Update Services for SAP Solutions: 8.1
Red Hat Enterprise Linux Server - Update Services for SAP Solutions: 8.4
Red Hat Enterprise Linux Server (for IBM Power LE) - Update Services for SAP Solutions: 8.1
Red Hat Enterprise Linux Server (for IBM Power LE) - Update Services for SAP Solutions: 8.4
Red Hat Enterprise Linux Server: 7
Red Hat Enterprise Linux Workstation: 7
Red Hat OpenShift Container Platform 4.9
Red Hat Software Collections: 1 for RHEL 7, 1 for RHEL 7.7
Red Hat Virtualization for IBM Power LE: 4
Red Hat Virtualization Host: 4
Red Hat Virtualization: 4
redhat-release-virtualization-host (Red Hat package): 4.3.4-1.el7ev, 4.3.5-2.el7ev, 4.3.5-4.el7ev, 4.3.6-2.el7ev, 4.3.6-5.el7ev, 4.3.9-2.el7ev, 4.3.11-1.el7ev, 4.3.12-4.el7ev, 4.3.13-2.el7ev, 4.3.14-2.el7ev, 4.3.16-1.el7ev, 4.3.17-1.el7ev, 4.3.18-1.el7ev
redhat-virtualization-host (Red Hat package): 4.3.11-20200922.0.el7_9, 4.3.12-20201216.0.el7_9, 4.3.13-20210127.0.el7_9, 4.3.14-20210322.0.el7_9, 4.3.16-20210615.0.el7_9, 4.3.17-20210713.0.el7_9, 4.3.18-20210903.0.el7_9
rh-redis5-redis (Red Hat package): before 5.0.5-3.el7

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

http://access.redhat.com/errata/RHSA-2021:3758
http://access.redhat.com/errata/RHSA-2021:3949
http://access.redhat.com/errata/RHSA-2021:3947
http://access.redhat.com/errata/RHSA-2021:3946
http://access.redhat.com/errata/RHSA-2021:3944
http://access.redhat.com/errata/RHSA-2021:3943
http://access.redhat.com/errata/RHSA-2021:3925
http://access.redhat.com/errata/RHSA-2021:3893
http://access.redhat.com/errata/RHSA-2021:3892
http://access.redhat.com/errata/RHSA-2021:3891
http://access.redhat.com/errata/RHSA-2021:3889
http://access.redhat.com/errata/RHSA-2021:3887
http://access.redhat.com/errata/RHSA-2021:3886
http://access.redhat.com/errata/RHSA-2021:3885
http://access.redhat.com/errata/RHSA-2021:3884

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.10.22 14:54:00 -03'00'