Alerta de seguridad cibernética	9VSA22-00624-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	27 de abril de 2022
Última revisión	27 de abril de 2022

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 CSIRT de Gobierno. 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 nuevas vulnerabilidades y actualizaciones de seguridad de Red Hat.

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

Vulnerabilidades

CVE-2022-29599
CVE-2021-44716
CVE-2022-21426
CVE-2022-21434
CVE-2022-21443
CVE-2022-21476
CVE-2022-21496
CVE-2021-4083
CVE-2022-0492
CVE-2022-25636
CVE-2021-4083
CVE-2022-0492
CVE-2022-21426
CVE-2022-21434
CVE-2022-21443
CVE-2022-21476
CVE-2022-21496
CVE-2022-25636
CVE-2022-22965
CVE-2021-4028
CVE-2021-4083
CVE-2021-20288
CVE-2021-43859
CVE-2021-45960
CVE-2021-46143
CVE-2022-0778
CVE-2022-22720
CVE-2022-22822
CVE-2022-22823
CVE-2022-22824
CVE-2022-22825
CVE-2022-22826
CVE-2022-22827
CVE-2022-23852
CVE-2022-25173
CVE-2022-25174
CVE-2022-25175
CVE-2022-25176
CVE-2022-25177
CVE-2022-25178
CVE-2022-25179
CVE-2022-25180
CVE-2022-25181
CVE-2022-25182
CVE-2022-25183
CVE-2022-25184
CVE-2022-25235
CVE-2022-25236
CVE-2022-25315
CVE-2022-0435
CVE-2022-0852

Impacto

Vulnerabilidades críticas:
CVE-2022-29599: Inyección de comandos via Commandline.

CVE-2021-44716: Error de consumo de recursos descontrolados en la biblioteca net/http de golang en la función canonicalHeader(). Su explotación puede llevar a denegación de servicio.

CVE-2022-25315: Un error en expat puede llevar a ejecución remota de código.

CVE-2022-25235: Un error en expat puede llevar a ejecución remota de código.

CVE-2022-25236: Un error en expat puede llevar a ejecución remota de código.

CVE-2022-22822: Un error en expat (libexpat) causa interrupción de procesos, y de ser explotado arriesgar la confidencialidad e integridad de los datos del sistema afectado.

CVE-2022-22823: Un error en expat (libexpat) causa interrupción de procesos, y de ser explotado arriesgar la confidencialidad e integridad de los datos del sistema afectado.

CVE-2022-22824: Un error en expat (libexpat) causa interrupción de procesos, y de ser explotado arriesgar la confidencialidad, disponibilidad e integridad de los datos del sistema afectado.

CVE-2022-23852: Un error en expat (libexpat) causa interrupción de procesos, y de ser explotado arriesgar la confidencialidad, disponibilidad e integridad de los datos del sistema afectado.

Productos afectados
Red Hat Enterprise Linux for Power, little endian: 7
Red Hat Enterprise Linux for Power, big endian: 7
Red Hat Enterprise Linux for IBM z Systems: 7
Red Hat Enterprise Linux for Scientific Computing: 7
Red Hat Enterprise Linux Desktop: 7
Red Hat Enterprise Linux Workstation: 7
Red Hat Enterprise Linux Server: 7
Red Hat Gluster Storage Web Administration (for RHEL Server) 3.1 x86_64
Red Hat OpenShift Container Platform 3.11 x86_64
Red Hat OpenShift Container Platform for Power 3.11 ppc64le
Red Hat OpenShift Container Platform 3.10 x86_64
Red Hat OpenShift Container Platform 3.9 x86_64
Red Hat OpenShift Container Platform 4.8 for RHEL 8 x86_64
Red Hat OpenShift Container Platform for Power 4.8 for RHEL 8 ppc64le
Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.8 for RHEL 8 s390x
Red Hat OpenShift Container Platform 4.8 for RHEL 8 x86_64
Red Hat OpenShift Container Platform for Power 4.8 for RHEL 8 ppc64le
Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.8 for RHEL 8 s390x

Red Hat OpenShift Container Platform 4.9 for RHEL 8 x86_64
Red Hat OpenShift Container Platform 4.8 for RHEL 8 x86_64
Red Hat OpenShift Container Platform 4.7 for RHEL 8 x86_64
Red Hat OpenShift Container Platform 4.6 for RHEL 8 x86_64
Red Hat OpenShift Container Platform for Power 4.9 for RHEL 8 ppc64le
Red Hat OpenShift Container Platform for Power 4.8 for RHEL 8 ppc64le
Red Hat OpenShift Container Platform for Power 4.7 for RHEL 8 ppc64le
Red Hat OpenShift Container Platform for Power 4.6 for RHEL 8 ppc64le
Red Hat Gluster Storage Web Administration (for RHEL Server) 3.1 x86_64
Red Hat JBoss Middleware Text-Only Advisories for MIDDLEWARE 1 x86_64
Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.1 ppc64le
Red Hat Enterprise Linux Server for x86_64 - Update Services for SAP Solutions 8.1 x86_64
Convert2RHEL 6 x86_64
Convert2RHEL 7 x86_64

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://access.redhat.com/security/cve/CVE-2022-29599
https://access.redhat.com/errata/RHSA-2022:1541
https://access.redhat.com/errata/RHBA-2022:1630
https://access.redhat.com/errata/RHBA-2022:1429
https://access.redhat.com/errata/RHBA-2022:1633
https://access.redhat.com/errata/RHSA-2022:1627
https://access.redhat.com/errata/RHSA-2022:1626
https://access.redhat.com/errata/RHBA-2022:1421
https://access.redhat.com/errata/RHSA-2022:1420
https://access.redhat.com/errata/RHSA-2022:1619
https://access.redhat.com/errata/RHSA-2022:1618
https://access.redhat.com/errata/RHSA-2022:1617
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29599
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44716
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21426
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21434
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21443
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21476
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21496
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4083
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0492
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25636
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4083
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0492
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21426
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21434

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21443
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21476
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21496
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25636
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22965
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4028
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4083
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-20288
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43859
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45960
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-46143
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0778
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22720
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22822
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22823
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22824
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22825
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22825
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22827
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23852
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25173
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25174
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25175
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25176
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25177
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25178
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25179
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25180
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25181
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25182
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25183
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25184
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25235
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25236
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25315
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0435
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0852

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.04.27 13:20:50 -04'00'