Alerta de Seguridad Cibernética

Alerta de seguridad cibernética	9VSA22-00630-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	6 de mayo de 2022
Última revisión	6 de mayo 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 conocidas para productos de Red Hat.

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

Vulnerabilidades

CVE-2022-29909
CVE-2022-29916
CVE-2022-29913
CVE-2022-29917
CVE-2022-29912
CVE-2022-1520
CVE-2022-29911
CVE-2022-29914
CVE-2022-1271

Impacto

Vulnerabilidades de riesgo alto

CVE-2022-29909: Permite a un atacante remoto evadir las restricciones de seguridad implementadas. Esta vulnerabilidad existe debido a una administración inapropiada de los permisos dentro de la aplicación.

CVE-2022-29917: La vulnerabilidad permite a un atacante remoto la ejecución arbitraria de código en el sistema objetivo. Existe debido a un error de límites de la memoria al procesar contenido HTML.

CVE-2022-1271: Esta vulnerabilidad permite a un atacante remoto comprometer el sistema afectado, y existe debido a una validación insuficiente al procesar nombres de archivo con dos o más newlines.

Productos afectados

Firefox (Red Hat package): 91.2.0-4.el8_1 - 91.8.0-1.el8_1
Firefox (Red Hat package): 91.4.0-1.el8_5 - 91.8.0-1.el8_5
gzip (Red Hat package): 1.9-10.el8_1 - 1.9-10.el8_2
Red Hat Enterprise Linux Desktop: 7
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: 8.4
Red Hat Enterprise Linux for IBM z Systems: 8
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 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 (for IBM Power LE) - Update Services for SAP Solutions: 8.1
Red Hat Enterprise Linux Server: 7
Red Hat Enterprise Linux Workstation: 7
thunderbird (Red Hat package): 91.2.0-1.el7_9 - 91.8.0-1.el7_9
Thunderbird (Red Hat package): 91.2.0-1.el8_1 - 91.8.0-1.el8_1
Thunderbird (Red Hat package): 91.2.0-1.el8_2 - 91.8.0-1.el8_2
Thunderbird (Red Hat package): 91.2.0-1.el8_4 - 91.8.0-1.el8_4
Thunderbird (Red Hat package): 91.4.0-2.el8_5 - 91.8.0-1.el8_5

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

http://access.redhat.com/errata/RHSA-2022:1727
http://access.redhat.com/errata/RHSA-2022:1726
http://access.redhat.com/errata/RHSA-2022:1725
http://access.redhat.com/errata/RHSA-2022:1730
http://access.redhat.com/errata/RHSA-2022:1724
http://access.redhat.com/errata/RHSA-2022:1705
http://access.redhat.com/errata/RHSA-2022:1704
http://access.redhat.com/errata/RHSA-2022:1703
http://access.redhat.com/errata/RHSA-2022:1702
http://access.redhat.com/errata/RHSA-2022:1701
http://access.redhat.com/errata/RHSA-2022:1676