Alerta de seguridad cibernética	9VSA21-00362-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de enero de 2021
Última revisión	13 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 89 vulnerabilidades que afectan a su producto Red Hat Quay.

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

Vulnerabilidades

CVE-2020-27831	CVE-2020-9803	CVE-2020-9862	CVE-2019-8743
CVE-2020-3899	CVE-2020-9806	CVE-2020-9850	CVE-2019-8720
CVE-2020-9802	CVE-2020-1752	CVE-2020-9843	CVE-2019-8710
CVE-2020-9327	CVE-2020-11793	CVE-2020-1971	CVE-2019-8625
CVE-2020-8492	CVE-2020-24659	CVE-2020-1751	CVE-2019-5018
CVE-2020-7595	CVE-2020-15503	CVE-2020-27832	CVE-2018-20843
CVE-2020-6405	CVE-2020-14422	CVE-2019-8782	CVE-2019-8819
CVE-2020-3902	CVE-2020-14391	CVE-2019-8816	CVE-2019-8823
CVE-2020-3901	CVE-2020-14382	CVE-2019-8815	CVE-2020-1730
CVE-2020-3900	CVE-2020-13632	CVE-2019-8814	CVE-2019-19906
CVE-2020-3897	CVE-2020-13631	CVE-2019-8813	CVE-2019-20916
CVE-2020-9805	CVE-2020-13630	CVE-2019-8812	CVE-2019-20907
CVE-2020-3895	CVE-2020-10029	CVE-2019-8811	CVE-2019-20807
CVE-2020-3894	CVE-2020-9807	CVE-2019-8808	CVE-2019-20454
CVE-2020-3885	CVE-2020-10018	CVE-2019-8783	CVE-2019-20388
CVE-2020-3868	CVE-2020-9925	CVE-2019-8771	CVE-2019-20387
CVE-2020-3867	CVE-2020-9915	CVE-2019-8820	CVE-2019-20218
CVE-2020-3865	CVE-2020-9895	CVE-2019-8769	CVE-2019-19956
CVE-2020-3864	CVE-2020-9894	CVE-2019-8766	CVE-2019-19221
CVE-2020-3862	CVE-2020-9893	CVE-2019-8764	CVE-2019-8835

CVE-2019-16935	CVE-2019-15165	CVE-2019-13050
CVE-2019-16168	CVE-2019-14889	CVE-2019-8846
CVE-2019-15903	CVE-2019-13627	CVE-2019-8844

Impacto

Entre las vulnerabilidades calificadas como de riesgo alto se encuentran las siguientes:

Errores de desbordamiento de buffer: CVE-2020-3899, CVE-2020-3900, CVE-2020-3895, CVE-2019-8782, CVE-2019-8816, CVE-2019-8815, CVE-2019-8814, CVE-2019-8811, CVE-2019-8812, CVE-2019-8808, CVE-2019-8783, CVE-2019-8820, CVE-2019-8766, CVE-2019-8743, CVE-2019-8720, CVE-2019-8710, CVE-2019-8819, CVE-2019-8823, CVE-2019-8835, CVE-2019-8844 y CVE-2020-3868 permiten a un atacante remoto ejecutar código arbitrario en el sistema. Un atacante remoto puede engañar a la víctima para que abra un archivo especialmente diseñado o visite una página maliciosa, gatillando corrupción de la memoria y ejecutando código arbitrario en el sistema objetivo.

CVE-2020-10029 permite a un atacante generar un desbordamiento del stack en buffer, que derive igualmente en el compromiso del sistema vulnerable o en condiciones de denegación de servicio.

Error de validación de entradas: CVE-2020-9802 y CVE-2020-9850 posibilitan a un atacante remoto ejecutar código arbitrario en el sistema objetivo, por culpa de una validación insuficiente de lo ingresado por el usuario al procesar contenido web. Gracias a eso, un atacante remoto puede crear una página web, engañar a la víctima para que la visite y ejecutar código arbitrario en su sistema.

Confusión de tipo de archivo: CVE-2020-3901 y CVE-2020-3897 hacen posible a un atacante remoto ejecutar código arbitrario en el sistema objetivo, debido a un error de confusión de tipo dentro del caché de transición de objetos. Un atacante remoto puede llevar a la víctima a visitar una página maliciosa o abrir un archivo especialmente diseñado, desatando un error de confusión de tipo de archivo y ejecutando código arbitrario en el sistema objetivo.

Corrupción de memoria: CVE-2020-9803, CVE-2020-9807 y CVE-2020-9806. Estas vulnerabilidades permiten a un atacante remoto ejecutar código arbitrario, debido a una validación insuficiente de las entradas entregadas por el usuario al procesar contenido web. Un atacante remoto puede engañar a la víctima para que abra un archivo especialmente diseñado o visite una página maliciosa, gatillando corrupción de la memoria y ejecutando código arbitrario en el sistema objetivo.

Escritura fuera de límites en memoria: CVE-2020-14382 y CVE-2020-1751. Permite a un atacante remoto no autenticado ejecutar código arbitrario.

CVE-2020-11793: Esta vulnerabilidad permite a un atacante remoto no autenticado ejecutar código arbitrario. Un problema de error de memoria después de ser liberada existe en WebKitGTK antes de la versión 2.28.1.

CVE-2020-1752: Error de memoria después de ser liberada permite a un usuario local escalar privilegios en el sistema. El error se encuentra dentro de la función glob() en glibc.

CVE-2019-8846: Error de memoria después de ser liberada en la función SVG Marker Element del WebKit de Safari de Apple. Un atacante remoto puede usar una web HTML diseñada especialmente, que al ser abierta por la víctima desate la corrupción de la memoria y la ejecución de código arbitrario.

CVE-2020-13630: Error de memoria después de ser liberada dentro de la función fts3EvalNextRow() en ext/fts3/fts3.c. Un atacante remoto puede enviar datos especialmente diseñados a la aplicación, detonando un error de memoria después de ser liberada y ejecutar código arbitrario en el sistema objetivo.

CVE-2020-10018, CVE-2020-9893 y CVE-2020-9895: Un atacante remoto puede engañar una víctima para que visite una web especialmente diseñada, detonando un error de memoria después de ser liberada y ejecutar código arbitrario en el sistema objetivo.

CVE-2019-5018: Esta vulnerabilidad permite a un atacante remoto comprometer al sistema vulnerable, debido a un error de memoria después de ser liberada dentro de la función ventana. El atacante puede enviar un comando SQL especialmente diseñado a la aplicación, detonando un error de memoria después de ser liberada y ejecutar código arbitrario en el sistema.

Productos afectados
Quay 3.3.0 y 3.3.1.

Mitigación
Instalar las actualizaciones desde el sitio del proveedor.

Enlaces
https://access.redhat.com/errata/RHSA-2021:0050

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27831

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3899

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9802

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9327

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8492

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7595

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6405

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3902

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3901

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3900

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3897

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9805

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3895

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3894

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3885

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3868

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3867

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3865

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3864

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3862

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9803

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9806

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1752

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11793

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24659

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15503

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14422

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14391

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14382

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13632

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13631

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13630

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10029

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9807

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10018

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9925

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9915

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9895

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9894

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9893

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9862

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9850

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9843

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1971

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1751

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27832

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8782

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8816

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8815

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8814

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8813

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8812

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8811

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8808

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8783

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8771

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8820

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8769

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8766

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8764

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8743

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8720

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8625

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5018

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-20843

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8819

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8823

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1730

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-19906

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-20916

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-20907

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-20807

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-20454

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-20388

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-20387

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-20218

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-19956

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-19221

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8835

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16935

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16168

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-15903

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-15165

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-14889

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-13627

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-13050

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8846

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8844