Alerta de seguridad cibernética	9VSA21-00381-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de febrero de 2021
Última revisión	02 de febrero 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 la información entregada por Apple, sobre 58 vulnerabilidades que afectan a varios de sus productos.
Este informe incluye las medidas de mitigación, consistentes en instalar las actualizaciones de los productos afectados.

Vulnerabilidades

CVE-2021-1761
CVE-2020-29614
CVE-2021-1793
CVE-2021-1737
CVE-2021-1738
CVE-2021-1744
CVE-2021-1779
CVE-2021-1757
CVE-2021-1764
CVE-2021-1750
CVE-2020-29633
CVE-2021-1771
CVE-2021-1762
CVE-2021-1763
CVE-2021-1774
CVE-2021-1767
CVE-2021-1745
CVE-2021-1753
CVE-2021-1768
CVE-2021-1751
CVE-2020-27938
CVE-2021-1769
CVE-2021-1788
CVE-2021-1765
CVE-2021-1801
CVE-2021-1789
CVE-2021-1799
CVE-2021-1777
CVE-2021-1754
CVE-2021-1797
CVE-2021-1790
CVE-2020-27945
CVE-2021-1760
CVE-2021-1747
CVE-2021-1776
CVE-2021-1759
CVE-2021-1772
CVE-2021-1792
CVE-2021-1787
CVE-2021-1786
CVE-2020-27937
CVE-2021-1802
CVE-2021-1791
CVE-2021-1775
CVE-2021-1746
CVE-2020-29608
CVE-2021-1758
CVE-2021-1783
CVE-2021-1741
CVE-2021-1743
CVE-2021-1773
CVE-2021-1778
CVE-2021-1736
CVE-2021-1785
CVE-2021-1766
CVE-2021-1818
CVE-2021-1742
CVE-2020-27904

Impacto

Las vulnerabilidades de alto riesgo son las siguientes.

CVE-2020-29614: Esta vulnerabilidad existe debido a un error de límites dentro del componente Model I/O en macOS. Un atacante remoto puede enviar un archivo especialmente diseñado, engañar a la víctima para que lo abra y provocar un desbordamiento del buffer y ejecutar código arbitrario en el sistema objetivo.
La explotación exitosa de esta vulnerabilidad puede comprometer completamente los sistemas vulnerables.

CVE-2021-1737, CVE-2021-1738, CVE-2021-1742, CVE-2021-1744, CVE-2021-1746, CVE-2021-1754, CVE-2021-1774, CVE-2021-1777 y CVE-2021-1793: Estas vulnerabilidades existen debido a una validación insuficiente de las entradas efectuadas por el usuario al procesar archivos de imágenes dentro del componente ImageIO en macOS. Un atacante remoto puede crear un archivo especialmente diseñado, engañar a la víctima para que lo abra y ejecutar código arbitrario en el sistema.

CVE-2021-1775: Esta vulnerabilidad existe debido a una validación insuficiente de las entradas efectuadas por el usuario al procesar archivos de fuentes dentro del componente FontParser en macOS. Un atacante remoto puede crear un archivo especialmente diseñado, engañar a la víctima para que lo abra y ejecutar código arbitrario en el sistema.

CVE-2021-1788: Esta vulnerabilidad existe debido a un error de uso de memoria después de ser liberada en WebKit. Un atacante remoto puede crear una página web especialmente diseñada, engañar a la víctima para que la abra y provocar un error de uso de memoria después de ser liberada y ejecutar código arbitrario en el sistema objetivo.

CVE-2021-1789: Esta vulnerabilidad existe debido a un error de confusión de tipo de archivo en WebKit. Un atacante remoto no autenticado puede crear una página web especialmente diseñada, engañar a la víctima para que la abra y provocar un error de uso de memoria después de ser liberada y ejecutar código arbitrario en el sistema objetivo.

CVE-2020-27945: Esta vulnerabilidad existe debido a un desbordamiento de enteros dentro del componente CFNetwork Cache en macOS. Un atacante remoto puede crear una página web especialmente diseñada, engañar a la víctima para que la abra y provocar un desbordamiento de enteros y ejecutar código arbitrario en el sistema objetivo.

CVE-2021-1760: Esta vulnerabilidad existe debido a un error de limites de la memoria dentro del componente CoreAnimation en macOS. Un atacante remoto puede crear un archivo especialmente diseñado, engañar a la víctima para que lo abra, detonar corrupción de memoria y ejecutar código arbitrario en el sistema.

CVE-2021-1772: Esta vulnerabilidad existe debido a un error de limites de la memoria dentro del componente CoreText en macOS. Un atacante remoto puede crear un archivo especialmente

diseñado, engañar a la víctima para que lo abra, detonar desbordamiento del stack en buffer y ejecutar código arbitrario en el sistema.

CVE-2021-1776: Esta vulnerabilidad existe debido a un error de límites al procesar fuentes dentro del componente CoreGraphics en macOS. Un atacante remoto puede crear un archivo o página web especialmente diseñada, engañar a la víctima para que lo abra y ejecutar código arbitrario en el sistema.

CVE-2021-1783 y CVE-2021-1818: Estas vulnerabilidades existen debido a un error de limites de la memoria dentro del componente ImageIO en macOS. Un atacante remoto puede crear un archivo especialmente diseñado, engañar a la víctima para que lo abra, detonar corrupción de memoria y ejecutar código arbitrario en el sistema.

Productos Afectados

macOS, versiones de la 10.15 a la 11.1.

Mitigación

Instalar las correspondientes actualizaciones desde el sitio del proveedor.

Enlaces

https://support.apple.com/en-us/HT212147

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1761

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-29614

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1793

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1737

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1738

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1744

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1779

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1757

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1764

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1750

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-29633

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1771

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1762

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1763

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1774

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1767

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1745

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1753

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1768

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1751

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27938

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1769

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1788

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1765

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1801

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1789

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1799

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1777

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1754

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1797

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1790

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27945

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1760

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1747

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1776

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1759

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1772

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1792

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1787

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1786

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27937

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1802

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1791

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1775

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1746

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-29608

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1758

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1783

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1741

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1743

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1773

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1778

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1736

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1785

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1766

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1818

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1742

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-279047523