Alerta de seguridad cibernética	9VSA20-00264-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de julio de 2020
Última revisión	09 de julio de 2020

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 obtenida de Huawei respecto a múltiples vulnerabilidades que afectan a sus productos. El presente informe incluye las respectivas medidas de mitigación.

Vulnerabilidades

CVE-2020-1838
CVE-2020-9263
CVE-2020-9262
CVE-2020-9261
CVE-2020-1839
CVE-2020-12695
CVE-2020-9100

CVE-2020-1838

Debido a que el dispositivo no valida suficientemente ciertas credenciales del rostro del usuario, un atacante con acceso local al dispositivo podría utilizar una credencial del usuario especialmente diseñada para evadir la autenticación.

Productos Afectados
Huawei Mate 30 Pro versiones anteriores a la 10.1.0.150(C00E136R5P3).

Mitigaciones
Actualizar a la versión 10.1.0.150(C00E136R5P3).

Enlaces
https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200701-03-smartphone-en
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1838

CVE-2020-9263

Existe una condición en la que el sistema podría referenciar memoria después de ser liberada, por lo que un atacante podría engañar a un usuario para instalar y ejecutar con privilegios especiales una aplicación especialmente diseñada, causar el error en memoria y lograr la ejecución de código en el sistema afectado.

Productos Afectados
Huawei Mate 30 versiones anteriores a la 10.1.0.150(C00E136R5P3).

Mitigaciones
Actualizar a la versión 10.1.0.150(C00E136R5P3).

Enlaces
https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200701-04-smartphone-en
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9263

CVE-2020-9262

Existe una condición en la que el sistema podría referenciar memoria después de ser liberada, por lo que un atacante podría engañar a un usuario para instalar y ejecutar con privilegios comunes una aplicación especialmente diseñada, causar el error en memoria y lograr la ejecución de código en el sistema afectado.

Productos Afectados

Huawei Mate 30 versiones anteriores a la 10.1.0.150(C00E136R5P3).

Mitigaciones
Actualizar a la versión 10.1.0.150(C00E136R5P3).

Enlaces
https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200701-05-smartphone-en
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9262

CVE-2020-9261

Debido a que el sistema no chequea y transforma correctamente el tipo de cierta variable, un atacante podría engañar a un usuario para instalar y ejecutar una aplicación especialmente diseñada y así lograr la ejecución de código en el sistema afectado.

Productos Afectados
Huawei Mate 30 versiones anteriores a la 10.1.0.150(C00E136R5P3).

Mitigaciones
Actualizar a la versión 10.1.0.150(C00E136R5P3).

Enlaces
https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200701-06-smartphone-en
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9261

CVE-2020-1839

Existe un lapso en el que ciertos punteros miembros pueden ser modificados por otro proceso que está operando concurrentemente. Un atacante podría engañar a un usuario para que ejecute una aplicación especialmente diseñada con privilegios especiales, explotar la vulnerabilidad de condición de carrera logrando ejecución de código.

Productos Afectados
Huawei Mate 30 versiones anteriores a la 10.1.0.150(C00E136R5P3).

Mitigaciones
Actualizar a la versión 10.1.0.150(C00E136R5P3).

Enlaces
https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200701-07-smartphone-en
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1839

CVE-2020-12695

Exite una vulnerabilidad en el protocolo UPnP que no prohibe la aceptación de una petición de subscripción con una URL de entrega en un segmento de red diferente que el completamente calificado para la subscripción de eventos, llamado "CallStranger". La función UPnP de los productos Huawei solo está activa en el lado de la LAN, y no en el lado de la WAN.

Productos Afectados
Huawei Mate 30 versiones anteriores a la 10.0.5.1(H612SP5C233).

Mitigaciones
Actualizar a la versión 10.0.5.1(H612SP5C233).

Enlaces
https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200701-01-upnp-en
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12695

CVE-2020-9100

Debido a la carga inapropiada de archivos DLL en el sistema de HiSuite, un atacante podría explotar esta vulnerabilidad para cargar un archivo DLL de su preferencia, logrando la ejecución de código en el sistema afectado.

Productos Afectados
HiSuite versiones anteriores a la 10.1.0.500.

Mitigaciones
Actualizar a la versión 10.1.0.500.

Enlaces
https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200701-01-dllhijacking-en
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9100