Alerta de seguridad cibernética	9VSA21-00350-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Bajo
TLP	Blanco
Fecha de lanzamiento original	5 de enero de 2021
Última revisión	5 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 Huawei sobre una serie de vulnerabilidades que afectan a algunos de sus productos.

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

Vulnerabilidades

CVE-2020-1866
CVE-2020-9203
CVE-2020-9209

CVE-2020-1866

Esta vulnerabilidad es categorizada como de riesgo bajo. CVE-2020-1866 permite a un atacante remoto realizar un ataque de denegación de servicio (DoS).

Productos Afectados

Huawei NIP6800: versiones V500R001C30, V500R001C60SPC500 y V500R005C00.
Huawei S12700, S5700, S2700, S7700 y S9700: versión V200R008C00.
Huawei Secospace USG6600: versiones V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500 y V500R005C00.
USG9500: V500R001C30SPC300, V500R001C30SPC600, V500R001C60SPC500 y V500R005C00.

Mitigación
Instalar las actualizaciones del sitio del proveedor.

Enlaces
https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-09-eudemon-en

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1866

CVE-2020-9203

Esta vulnerabilidad es categorizada como de riesgo bajo. CVE-2020-9203 permite a una aplicación local realizar un ataque de denegación de servicio (DoS).

Productos Afectados
Huawei P30.

Mitigación
Instalar las actualizaciones del sitio del proveedor.

Enlaces
https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20201230-01-resourcemanagement-en

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9203

CVE-2020-9209

Esta vulnerabilidad es categorizada como de riesgo bajo. CVE-2020-9209 permite a un usuario local escalar privilegios en el sistema.

Productos Afectados
Huawei SMC2.0, versiones V600R006C00SPC700, V600R006C00SPC800, V600R006C10SPC500, V600R006C10SPC600, V600R006C10SPC601, V600R006C10SPC602, V600R006C10SPC700, V600R006C10SPC800, V600R006C10SPCa00, V600R006C10SPCb00, V600R006C10SPCc00, V600R006C10SPCd00, V600R006C10SPCe00, V600R019C00 y V600R019C10.

Mitigación
Instalar las actualizaciones del sitio del proveedor.

Enlaces
https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20201230-01-pe-en

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9209