Alerta de Seguridad Informática (9VSA-00022-001)

Nivel de Riesgo: Alto

Tipo: Vulnerabilidad

Fecha de lanzamiento original: 22 de Julio de 2019 | Última revisión 22 de Julio de 2019

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 liberado por Cisco sobre tres actualizaciones de seguridad para abordar vulnerabilidades con clasificación alta y crítica. Un atacante podría explotar algunas de estas vulnerabilidades para tomar el control de un sistema afectado o bien realizar ataques de denegación de servicio.

Vulnerabilidad

CVE-2019-1920
CVE-2019-1919
CVE-2019-1917

Impacto

CVE-2019-1920

Una vulnerabilidad en 802.11r Fast Transition para Cisco IOS Access Points presente en la implementación del manejo de errores para las solicitudes de autenticación de clientes podría causar una denegación de servicio (reinicio inesperado del dispositivo) ante la recepción de solicitudes de autenticación por parte de un atacante no autenticado en red adyacente.

CVE-2019-1919

Una vulnerabilidad en las imágenes de la máquina virtual (VM) en Cisco FindIT Network Management Software podría permitir que un atacante local no autenticado que tenga acceso a la consola de la máquina virtual inicie sesión en el dispositivo con una cuenta estática que tenga privilegios de raíz.

CVE-2019-1917

Una vulnerabilidad en la interfaz de la API REST de Cisco Vision Dynamic Signage Director podría permitir que un atacante remoto no autenticado omita la autenticación en un sistema afectado.

Productos afectados

CVE-2019-1920: Cisco IOS Access Point Software configurado para 802.11r FT.

CVE-2019-1919: Cisco FindIT Network Manager y Cisco FindIT Network Probe versión 1.1.4

CVE-2019-1917: Cisco Vision Dynamic Signage Director

Mitigación

Se recomienda actualizar los productos afectados de manera urgente, siguiendo los pasos provistos por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190717-aironet-dos

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190717-cfnm-statcred

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190717-cvdsd-wmauth

Contactos

https://www.csirt.gob.cl
+ (562) 24863850
@CSIRTGOB
https://www.linkedin.com/company/csirt-gob

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.07.22 17:00:30 -04'00'