Alerta de seguridad informática	9VSA20-00115-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de enero de 2020
Última revisión	09 de enero 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 entregada por Fortinet referente a diversas vulnerabilidades que afectan a la implementación estandar de FortiOS y FortiAP-S/W2. El informe contiene la correspondiente mitigación.

Vulnerabilidad

CVE-2019-9494
CVE-2019-9495
CVE-2019-9496
CVE-2019-9497
CVE-2019-9498
CVE-2019-9499

Impacto

Existen múltiples vulnerabilidades, denominadas Dragonblood, en la implementación estándar WiFi WPA3. Estas vulnerabilidades pueden causar la fuga de contraseña, la denegación de servicio o la omisión de autorización.

CVE-2019-9494
Ataque de caché SAE contra grupos ECC (ataques de canal lateral SAE)

CVE-2019-9495
Ataque de caché EAP-PWD contra grupos ECC (ataque de canal lateral EAP-PWD)

CVE-2019-9496
SAE confirma la validación del estado faltante

CVE-2019-9497
Ataque de reflexión EAP-PWD (validación de confirmación faltante de EAP-PWD)

CVE-2019-9498
Falta la validación de confirmación del servidor EAP-PWD

CVE-2019-9499
Validación de confirmación de falta de par EAP-PWD

Productos Afectados

FortiOS, versiones anteriores a 6.2.2
FortiAP-S/W2, versiones anteriores a 6.2.1
Meru AP, versiones anteriores a 8.5.1
Meru Controller, versiones anteriores a 8.5.1

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://fortiguard.com/psirt/FG-IR-19-107
https://kb.cert.org/vuls/id/871675/