ALERTA: VULNERABILIDADES EN PRODUCTOS DE SEGURIDAD CISCO (29/OCTUBRE/2021)

Atacantes podrían explotar vulnerabilidades en productos de seguridad CISCO y tomar control total de las comunicaciones de los sistemas afectados.

Introducción

CISCO ASA Adaptative Security Applicance es un dispositivo de gestión integral que combina varias funcionalidades de seguridad, tales como Firewall, Antivirus, Prevención de Intrusos y Redes Virtuales Privadas. Este dispositivo analiza las conexiones hacia la red protegida a fin de prevenir tanto la infección como comprometimiento de los activos de información.

Un error en el proceso de identificación de roles en el Firewall tanto para los módulos ASA y FTD debido a una gestión inadecuada de requerimientos de servicios de red, provocaría que usuarios no autenticadados, ataquen de manera remota a los sistemas, pasando por alto las protecciones de seguridad.

En consideración alto riesgo contra la confidencialidad, integridad y disponibilidad de los activos de información protegidos por los dispositivos de seguridad CISCO ASA y FTD, el EcuCERT de ARCOTEL recomienda a su comunidad objetivo, tomar en consideración las siguientes recomendaciones:

1. Actualizar la versión de software y firmware de los dispositivos CISCO según las instrucciones del fabricante.

2. Considerar las recomendaciones para acciones temporales de mitigación emitidas por el fabricante.

3. Implementar acciones de control a fin de identificar conexiones atípicas hacia la red organizacional protegida.

4. Asegurarse que los perfiles de usuarios internos de la red, estén definidos bajo el principio del menor privilegio posible.

Referencias

- CISCO (2021). Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Identity-Based Rule Bypass Vulnerability. Disponible en https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rule-bypass-ejjOgQEY
- CISCO (2021). Cisco Security Advisories. Disponible en https://tools.cisco.com/security/center/publicationListing.x
- CVE (2021). CVE-2021-34787. Disponible en https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rule-bypass-ejjOgQEY
- CISCO (2021). Cisco Event Response: October 2021 Cisco ASA, FMC, and FTD Software Security Advisory Bundled Publication. Disponible en https://tools.cisco.com/security/center/viewErp.x?alertId=ERP-74773