Centro Nacional de Seguridad Digital	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 117**	**Fecha: 20-05-2023**
		Página 4 de 11

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Las fallas críticas en los switches de Cisco para pequeñas empresas podrían permitir ataques remotos		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet, Correo electrónico, entre otros.		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

Cisco ha lanzado actualizaciones para abordar un conjunto de nueve fallas de seguridad en sus conmutadores de la serie Small Business que podrían ser explotados por un atacante remoto no autenticado para ejecutar código arbitrario o causar una condición de denegación de servicio (DoS).

DETALLES:

- Estas vulnerabilidades se deben a la validación incorrecta de las solicitudes que se envían a la interfaz web.
- Cuatro de las nueve vulnerabilidades tienen una calificación de 9,8 sobre 10 en el sistema de calificación CVSS, lo que las convierte en críticas por naturaleza. Los nueve defectos afectan a las siguientes líneas de productos:
  - Conmutadores inteligentes de la serie 250 (corregidos en la versión de firmware 2.5.9.16)
  - Switches administrados de la serie 350 (corregidos en la versión de firmware 2.5.9.16)
  - Switches administrados apilables de la serie 350X (corregidos en la versión de firmware 2.5.9.16)
  - Switches administrados apilables de la serie 550X (corregidos en la versión de firmware 2.5.9.16)
  - Conmutadores inteligentes de la serie Business 250 (corregidos en la versión de firmware 3.3.0.16)
  - Conmutadores gestionados de la serie Business 350 (corregidos en la versión de firmware 3.3.0.16)
  - Conmutadores inteligentes de la serie 200 para pequeñas empresas (no se parchearán)
  - Conmutadores administrados de la serie 300 para pequeñas empresas (no se parchearán)
  - Conmutadores administrados apilables de la serie 500 para pequeñas empresas (no se aplicarán parches)
- Una breve descripción de cada uno de los defectos es la siguiente:
  - CVE-2023-20159 (puntuación CVSS: 9,8): Vulnerabilidad de desbordamiento del búfer de pila de los switches Cisco Small Business Series
  - CVE-2023-20160 (puntuación CVSS: 9,8): Vulnerabilidad de desbordamiento de búfer BSS no autenticado de Cisco Small Business Series Switches
  - CVE-2023-20161 (puntuación CVSS: 9,8): Vulnerabilidad de desbordamiento de búfer de pila no autenticado de Cisco Small Business Series Switches
  - CVE-2023-20189 (puntuación CVSS: 9,8): Vulnerabilidad de desbordamiento de búfer de pila no autenticado de Cisco Small Business Series Switches
  - CVE-2023-20024 (puntuación CVSS: 8,6): Vulnerabilidad de desbordamiento de búfer de almacenamiento dinámico no autenticado de Cisco Small Business Series Switches
  - CVE-2023-20156 (puntuación CVSS: 8,6): Vulnerabilidad de desbordamiento de búfer de almacenamiento dinámico no autenticado de Cisco Small Business Series Switches
  - CVE-2023-20157 (puntuación CVSS: 8,6): Vulnerabilidad de desbordamiento de búfer de almacenamiento dinámico no autenticado de Cisco Small Business Series Switches
  - CVE-2023-20158 (puntuación CVSS: 8,6): Vulnerabilidad de denegación de servicio no autenticada de Cisco Small Business Series Switches
  - CVE-2023-20162 (puntuación CVSS: 7,5): Vulnerabilidad de lectura de configuración no autenticada de Cisco Small Business Series Switches
- La explotación exitosa de los errores antes mencionados podría permitir que un atacante remoto no autenticado ejecute código arbitrario con privilegios de raíz en un dispositivo afectado mediante el envío de una solicitud especialmente diseñada a través de la interfaz de usuario basada en la web.

- Alternativamente, también se podría abusar de ellos para desencadenar una condición DoS o leer información no autorizada en sistemas vulnerables por medio de una solicitud maliciosa.

RECOMENDACIONES:

- Cisco ya no planea lanzar actualizaciones de firmware para Small Business 200 Series Smart Switches, Small Business 300 Series Managed Switches, Small Business 500 Series Stackable Managed Switches, ya que han entrado en el proceso de fin de vida útil.
- Aplicar los parches de seguridad para mitigar las vulnerabilidades.

Fuentes de información	▪ hxxps://thehackernews.com/2023/05/critical-flaws-in-cisco-small-business.html ▪ Análisis propio de fuentes abiertas.