	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 150		Fecha: 26-06-2023
			Página 8 de 37
Componente que reporta	**CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	Fortinet publica avisos de seguridad para fallas en FortiNAC		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

ANTECEDENTES:

El 21 de junio del 2023, a través del monitoreo y búsqueda de amenazas en el ciberespacio, Fortinet ha publicado 2 nuevos avisos de seguridad, entre ellos se contemplan 2 vulnerabilidades clasificadas en 1 Crítica y 1 Media.

DETALLES:

Severidad crítica CVE-2023-33299 [CVSSv3: 9.6] FortiNAC. Una deserialización de una vulnerabilidad de datos no confiables en FortiNAC puede permitir que un usuario no autenticado ejecute códigos o comandos no autorizados a través de solicitudes diseñadas específicamente para el servicio tcp/1050.

Severidad media CVE-2023-33300 [CVSSv3: 4.8] FortiNAC: inyección de argumentos en la interfaz XML en el puerto tcp/5555. Una neutralización incorrecta de elementos especiales utilizados en un comando ('inyección de comando') puede permitir a un atacante no autenticado copiar archivos locales del dispositivo a otros directorios locales del dispositivo a través de campos de entrada especialmente diseñados. Para acceder a los datos copiados, sin embargo, el atacante debe tener un punto de acceso ya existente en el dispositivo con privilegios suficientes.

Productos afectados. FortiNAC versión 9.4.0 a 9.4.2, FortiNAC versión 9.2.0 a 9.2.7, FortiNAC versión 9.1.0 a 9.1.9, FortiNAC versión 7.2.0 a 7.2.1, FortiNAC 8.8 todas las versiones, FortiNAC 8.7 todas las versiones, FortiNAC 8.6 todas las versiones, FortiNAC 8.5 todas las versiones, FortiNAC 8.3 todas las versiones.

RECOMENDACIONES:

- Instalar la actualización de los fabricantes disponibles en páginas oficiales del proveedor.
- Actualizar a FortiNAC versión 9.4.3 o superior.
- Actualizar a FortiNAC versión 9.2.8 o superior.
- Actualizar a FortiNAC versión 9.1.10 o superior

Fuentes de información	• hxxps://portal.cci-entel.cl/Threat_Intelligence/Boletines/1634/ • hxxps://www.fortiguard.com/psirt/FG-IR-23-074

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 150	**Fecha: 26-06-2023**
		Página 9 de 37

Componente que reporta	**CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	Los piratas informáticos secuestran los sistemas Linux utilizando la versión troyana de OpenSSH		
Tipo de Ataque	Troyanos	Abreviatura	Troyanos
Medios de propagación	USB, Disco, Red, Correo, Navegación de internet		
Código de familia	C	Código de Sub familia	C02
Clasificación temática familia	Código Malicioso		

Descripción

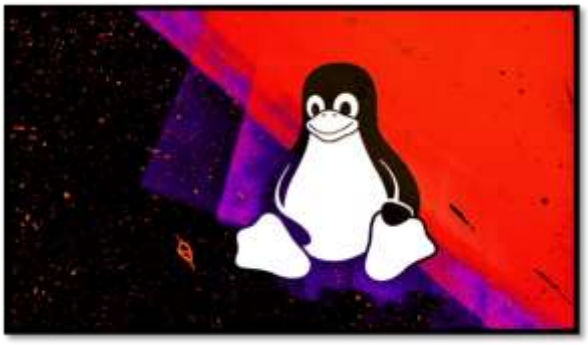
ANTECEDENTES:

El 24 de junio del 2023, a través del monitoreo y búsqueda de amenazas en el Ciberespacio, se tiene conocimiento que los dispositivos Linux e Internet de las cosas (IoT) expuestos a Internet están siendo secuestrados en ataques de fuerza bruta.

DETALLES:

Después de obtener acceso a un sistema, los atacantes implementan un paquete OpenSSH con troyanos que les ayuda a acceder a los dispositivos comprometidos y robar las credenciales de SSH para mantener la persistencia, duplicando el binario en varias ubicaciones de disco y creando trabajos cron para ejecutarlo periódicamente. Además, registra ZiggyStarTux como un servicio de systemd, configurando el archivo de servicio en /etc/systemd/system/network-check.service.

También se configuraba a los bots para que descargaran y ejecutaran scripts de shell adicionales para aplicar fuerza bruta a cada host en la subred del dispositivo pirateado y la puerta trasera en cualquier sistema vulnerable que usara el paquete OpenSSH troyano.



El script de shell de puerta trasera implementado al mismo tiempo que el binario OpenSSH troyano agregará dos claves públicas al archivo authorized_keys para acceso SSH persistente, permite a los actores de amenazas recolectar información del sistema e instalar los rootkits.

Después de moverse lateralmente dentro de la red de la víctima, el objetivo final de los atacantes parece ser la instalación de malware de minería dirigido a sistemas Hiveon OS basados en Linux diseñados para criptominería.

RECOMENDACIONES:

- Descargar software del sitio oficial de su distribución.
- Evitar conexión con contraseña vacía.
- Configurar la autenticación de clave pública.

Fuentes de información	• hxxps://www.bleepingcomputer.com/news/security/microsoft-hackers-hijack-linux-systems-using-trojanized-openssh-version/?&web_view=true • hxxps://www.calcomsoftware.com/configuracion-de-ssh-para-una-mejora-en-su-seguridad