	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°148	Fecha: 24-06-2023
		Página: 5 de 14

Componente que reporta	**COMANDO OPERACIONAL DE CIBERDEFENSA DEL COMANDO CONJUNTO DE LAS FUERZAS ARMADAS**		
Nombre de la alerta	La vulnerabilidad de los equipos de Microsoft permite que los atacantes entreguen malware desde cuentas externas		
Tipo de Ataque	Malware	Abreviatura	Malware
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

1. Microsoft Teams es utilizado por más de 280 millones de usuarios activos cada mes y es una forma popular para que las organizaciones hablen y trabajen juntas usando Microsoft 365.

La explotación exitosa de esta vulnerabilidad permite a los actores de amenazas evadir los controles de seguridad del lado del cliente. Esta característica de seguridad prohíbe que los usuarios fuera de la organización envíen cualquier archivo a los usuarios internos de la organización.

Corbridge afirmó en un informe que el puente de comunicación que descubrieron es más vital porque puede enviar material dañino directamente al correo electrónico de alguien, lo cual es más potente que simplemente engañarlo, aparte de esto, dos miembros del Equipo Rojo de Jumpsec descubrieron una solución para eludir la limitación existente.
Hicieron esto alterando la identificación del destinatario en la solicitud POST de un mensaje para destinatarios internos y externos, engañando así al sistema para que reconociera a un usuario externo como un usuario interno.

En ensayos pragmáticos, los investigadores aplicaron la técnica. Se infiltraron con éxito en una carga útil de comando y control en la bandeja de entrada de una organización objetivo, todo mientras operaban de manera encubierta como parte de su ejercicio de equipo rojo.

Los atacantes infectan fácilmente a las organizaciones que usan Microsoft Teams al pasar por alto las medidas de seguridad y la capacitación antiphishing , explotando la configuración predeterminada de la misma. Al registrar un dominio similar al Microsoft 365 del objetivo, el atacante puede crear mensajes que parecen internos en lugar de externos, lo que aumenta la posibilidad de que el objetivo descargue el archivo sin sospechar.

Los investigadores notificaron a Microsoft sus hallazgos, esperando una respuesta inmediata debido al considerable impacto observado, a pesar de que Microsoft reconoció la existencia de la falla, su respuesta indicó que no alcanza el umbral para una acción inmediata, lo que implica una falta de urgencia para abordar el problema, para minimizar el riesgo, las organizaciones que utilizan Microsoft Teams sin requerir una comunicación regular con usuarios externos deben deshabilitar esta función.

Para hacer esto, debe seguir los sencillos pasos que mencionamos a continuación:

- En primer lugar, vaya al Centro de administración de Microsoft Teams.
- Luego acceda a la opción Acceso Externo.
- Después de eso, debe deshabilitar el chat con usuarios externos de Teams no administrados.
- Las organizaciones pueden establecer una lista de permitidos para dominios específicos para mitigar los riesgos de explotación al mantener canales de comunicación externos.

2. Recomendaciones

- Instala un software antivirus/malware.
- Mantén actualizado tu software antivirus.
- Ejecuta análisis programados regularmente con tu software antivirus.
- Mantén tu sistema operativo actualizado.
- Protege tu red.

Fuente de Información:	hxxps://gbhackers.com/microsoft-teams-vulnerability/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 148	Fecha: 24-06-2023
		Página 9 de 14

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades críticas en FortiNAC de Fortinet		
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

1. ANTECEDENTES

Fortinet ha reportado múltiples vulnerabilidades de severidad CRÍTICA y MEDIA de tipo deserialización de datos no confiables e inyección de comandos en aplicaciones FortiNAC. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto ejecutar código arbitrario en el sistema de destino y manipular archivos en el dispositivo.

2. DETALLES

- **FortiNAC** es una solución de acceso de confianza cero de **Fortinet** que supervisa y protege todos los activos digitales conectados a la red empresarial, cubriendo dispositivos que van desde TI, IoT, OT/ICS hasta IoMT. FortiNAC proporciona protección contra amenazas de IoT, extiende el control a dispositivos de red de terceros y organiza la respuesta automática a una amplia gama de eventos de red.
- La vulnerabilidad registrada con el código CVE-2023-33299 de severidad **crítica** de tipo deserialización de datos no confiables, existe debido a una validación de entrada insegura al procesar datos serializados. Un atacante remoto puede enviar una solicitud especialmente diseñada al puerto 1050/TCP y ejecutar código arbitrario en el sistema de destino.
- La vulnerabilidad registrada con el código CVE-2023-33300 de severidad **media** de tipo inyección de comandos, existe debido a una validación de entrada incorrecta al procesar solicitudes enviadas a la interfaz XML en el puerto 5555/TCP. Un atacante remoto no autenticado puede enviar una solicitud especialmente diseñada al sistema y copiar archivos locales del dispositivo a otros directorios locales del dispositivo. Sin embargo, para acceder a los datos copiados, el atacante debe tener un punto de apoyo ya existente en el dispositivo con suficientes privilegios.

A. Productos afectados:

- FortiNAC: 9.4.0 – 9.4.3;
- 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;
- FortiNAC-F: 7.2.0 – 7.2.1.

3. RECOMENDACIONES:

- Se recomienda actualizar los productos afectados con la última versión de software disponible desde el sitio web del proveedor que aborda estas vulnerabilidades.

Fuente de Información:	• hxxps://fortiguard.fortinet.com/psirt/FG-IR-23-096 • hxxps://fortiguard.fortinet.com/psirt/FG-IR-23-074