DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 139**	**Fecha: 14-06-2023**
		Página 6 de 11

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**			
Nombre de la alerta	Fortinet lanza parche que corrige una vulnerabilidad crítica de RCE en FortiOS SSL VPN			
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. Resumen:

Se ha reportado múltiples vulnerabilidades de severidad **ALTA** de tipo información insuficiente en Golang que afecta a IBM Db2 REST. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto inyectar código HTML malicioso y comprometer el sistema vulnerable. Fortinet ha lanzado parches para abordar una vulnerabilidad de severidad **CRÍTICA** de tipo desbordamiento de búfer de almacenamiento dinámico en la autenticación previa en FortiOS y FortiProxy SSL-VPN. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto la ejecución remota de código en dispositivos SSL VPN y la pérdida de datos y corrupción de archivos y SO.

1. Detalles:

- La vulnerabilidad de severidad **CRÍTICA** registrada con el código CVE-2023-27997 de tipo desbordamiento de búfer basada en montón en FortiOS versión 7.2.4 y anteriores, versión 7.0.11 y posteriores, versión 6.4.12 y posteriores, versión 6.0.16 y posteriores y FortiProxy versión 7.2.3 y posteriores, versión 7.0.9 y anteriores, versión 2.0.12 y posteriores, versión 1.2 todas las versiones, versión 1.1 todas las versiones SSL-VPN puede permitir que un atacante remoto ejecute código o comandos arbitrarios a través de solicitudes diseñadas específicamente.
- Los investigadores de Fortinet señalaron además que, de acuerdo a una investigación realizada, se ha identificado que la campaña "Volt Typhoon" utiliza una variedad de tácticas, técnicas y procedimientos (TTP) para obtener acceso a las redes, incluida una técnica ampliamente utilizada conocida como "**vivir de la tierra**" para evadir la detección. La campaña parece explotar vulnerabilidades para las que existen parches, principalmente FG-IR-22-377 / CVE-2022-40684 para el acceso inicial, como indicadores de compromiso: nombre de cuentas de administrador "fortinet-tech-support" y "fortigate-tech- support" se encontraron en los dispositivos de los clientes relacionados con esta campaña.
- Es por ello, que por ahora no se ha vinculado la vulnerabilidad FG-IR-23-097 con la campaña **Volt Typhoon**, sin embargo, Fortinet espera que todos los actores de amenazas, incluidos los que están detrás de la campaña **Volt Typhoon**, continúen explotando vulnerabilidades sin parches en software y dispositivos ampliamente utilizados. Por esta razón, Fortinet insta a la mitigación inmediata y continua a través de una campaña agresiva de parches.

2. Productos afectados:

- FortiOS versión 7.2.4 y anteriores, versión 7.0.11 y posteriores, versión 6.4.12 y posteriores, versión 6.0.16 y posteriores y FortiProxy versión 7.2.3 y posteriores, versión 7.0.9 y anteriores, versión 2.0.12 y posteriores, versión 1.2 todas las versiones, versión 1.1 todas las versiones SSL-VPN.

3. Solución:

- Fortinet recomienda actualizar los productos afectados con la última versión de firmware más recientes que abordan estas vulnerabilidades;
- Como solución alterna, Fortinet recomienda deshabilitar el módulo SSL-VPN. Si el cliente no está operando SSL-VPN, el riesgo de este problema se mitiga; sin embargo, Fortinet aún recomienda actualizar;
- Asimismo, se recomienda revisar los sistemas en busca de evidencia de explotación de vulnerabilidades anteriores, por ejemplo, FG-IR-22-377 / CVE-2022-40684;
- Mantener una buena higiene cibernética y seguir las recomendaciones de parches del proveedor;

- Seguir las recomendaciones de endurecimiento, por ejemplo, la Guía de endurecimiento de FortiOS 7.2.0;
- Minimizar la superficie de ataque desactivando funciones no utilizadas y administrando dispositivos a través de un método fuera de banda siempre que sea posible.

Fuente de Información:	• hxxps://www.fortinet.com/blog/psirt-blogs/analysis-of-cve-2023-27997-and-clarifications-on-volt-typhoon-campaign • hxxps://fortiguard.com/psirt/FG-IR-23-097 • hxxps://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 139**	**Fecha: 14-06-2023**
		Página 8 de 11

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades en Microsoft Windows Pragmatic General Multicast		
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. Resumen:

Se ha reportado múltiples vulnerabilidades de severidad **ALTA** de tipo error de validación de entrada, en Microsoft Windows Pragmatic General Multicast (PGM). La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto ejecutar código arbitrario en el sistema vulnerable.

2. Detalles:

- La vulnerabilidad registrada con el código CVE-2023-32015, CVE-2023-29363 y CVE-2023-32014 de severidad **alta** de tipo error de validación de entrada, existen debido a una validación insuficiente de la entrada proporcionada por el usuario en Windows Pragmatic General Multicast (PGM). Un atacante remoto puede enviar un archivo especialmente diseñado y ejecutar código arbitrario en el sistema de destino.
- El producto no puede realizar una verificación adecuada de la entrada. Dichos problemas pueden influir en el manejo del flujo de datos del programa. En caso de ausencia de una verificación de entrada adecuada, los atacantes pueden crear e ingresar datos que provocan cambios en el flujo de control, control arbitrario de un recurso o ejecución de código arbitrario.

3. Productos afectados:

- Windows: 10 - 11 22H2;
- Windows Server: 2008 - 2022 20H2.

4. Solución:

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

Fuentes de información	hxxps://www.ibm.com/support/pages/node/7001723