PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno y Transformación Digital

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Asociación de Bancos del Perú

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

180-2024-CNSD

La presente **Alerta Integrada de Seguridad Digital** corresponde a un análisis técnico periódico realizado por el Comando Conjunto de las Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aéreadel Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en el marco de la Seguridad Digital del Estado Peruano.

El objetivo de esta alerta **es informar a los responsables de la seguridad digital de las entidades públicas y lasempresas privadas sobre las amenazas en el entorno digital** para advertir las situaciones que pudieran afectar la continuidad de sus servicios en favor de la población.

Las marcas y logotipos de empresas privadas y/o entidades públicas se reflejan para ilustrar la información que los ciudadanos reciben por redes sociales u otros medios y que atentan contra la confianza digital de las personas y de las mismas empresas **de acuerdo con lo establecido por el Decreto de Urgencia 007-2020**.

La presente Alerta Integrada de Seguridad Digital es información netamente especializada para informar a las áreas técnicas de entidades y empresas.

Contenido

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°180	Fecha: 05-08-2024
		Página: 4 de 8

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	El APT StormBamboo ataca a los ISP y propaga malware mediante actualizaciones de software		
Tipo de Ataque	Amenaza Avanzada Persistente	Abreviatura	APT
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Sub familia	G02
Clasificación temática familia	Fraude		

Descripción

1. ANTECEDENTES:

La empresa de inteligencia de amenazas Volexity ha revelado que un actor de amenazas chino está utilizando envenenamiento de DNS a nivel de ISP para enviar malware contra sus objetivos. El actor APT rastreado como StormBamboo es conocido por sus operaciones de ciberespionaje dirigidas a organizaciones asiáticas. El grupo ha dominado el arte de explotar a terceros, como los ISP, para lanzar ataques posteriores.

2. DETALLES:

Su último plan implica manipular mecanismos de actualización de software inseguros para inyectar malware silenciosamente en las máquinas de víctimas desprevenidas.

StormBamboo estaba alterando las respuestas de las consultas DNS para los dominios vinculados a los mecanismos de actualización automática de software. Los atacantes atacaron el software mediante mecanismos de actualización inseguros como HTTP y no pudieron validar las firmas digitales de los instaladores, lo que provocó la instalación de malware en lugar de las actualizaciones previstas.

El ataque se basa en una técnica conocida como man-in-the-middle (MITM), en la que los atacantes se colocan básicamente entre un dispositivo objetivo y un servidor de confianza. Esto les permite interceptar y manipular la comunicación que fluye entre las dos partes.

En el caso del ISP comprometido, los atacantes pudieron envenenar las solicitudes DNS, una función crítica que traduce las direcciones de sitios web en direcciones IP numéricas. Al manipular las respuestas DNS, los atacantes podían redirigir a los usuarios a sitios web maliciosos diseñados para robar información confidencial. Además, se ha observado que StormBamboo implementa una extensión de navegador maliciosa llamada RELOADEXT, probablemente diseñada para manipular resultados de búsqueda o inyectar anuncios en sesiones de navegación web.

El ISP, al descubrir la vulnerabilidad, tomó medidas rápidas para mitigar el daño con la ayuda de Volexity. Se reiniciaron los dispositivos de red clave, lo que interrumpió de manera efectiva la operación MitM de los atacantes. Sin embargo, los atacantes ya habían aprovechado la interrupción para implementar malware que roba información en dispositivos desprevenidos.

IOCs:

- Servidor C2 utilizado durante el envenenamiento de DNS: 103.96.130.107
- Servidor MACMA C2: 152.32.159.8
- CATCHDNS C2: 122.10.90.20
- CATCHDNS C2: 122.10.89.110
- CATCHDNS C2: 59.188.69.231

3. RECOMENDACIÓN:

- Bloquear los IOC proporcionados listados.

Fuente de Información:	• hxxps://hackread.com/stormbamboo-apt-isps-malware-via-software-updates/ • hxxps://www.volexity.com/blog/2024/08/02/stormbamboo-compromises-isp-to-abuse-insecure-software-update-mechanisms/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°180	Fecha: 05-08-2024
		Página: 5 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades en los chipsets de MediaTek		
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:

Se ha reportado dos vulnerabilidades de severidad **ALTA** de tipo corrupción de memoria y escritura fuera de límites que afecta a los chipsets de MediaTek. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto / local la ejecución de código arbitrario.

2. DETALLES:

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2024-20082 de tipo corrupción de memoria, podría permitir a un atacante remoto no autenticado ejecutar código arbitrario. La vulnerabilidad existe debido a que falta una verificación de límites en el módem. Un atacante remoto puede engañar a la víctima para que abra un archivo especialmente diseñado y ejecute código arbitrario.

La vulnerabilidad de severidad **baja**, identificada por MITRE como CVE-2024-20083 de tipo escritura fuera de límites, permite que una aplicación privilegiada local ejecute código arbitrario. La vulnerabilidad existe debido a una falta de verificación de límites dentro de VENC. Una aplicación local privilegiada puede ejecutar código arbitrario. Esta vulnerabilidad puede explotarse localmente. El atacante debe tener credenciales de autenticación y autenticarse correctamente en el sistema.

A. Productos afectados:

- La vulnerabilidad CVE-2024-20082 a todas las versiones de chipsets de la serie: MT2735, MT2737, MT6833, MT6835, MT6835T, MT6853, MT6855, MT6873, MT6875, MT6875T, MT6877, MT6879, MT6880, MT6883, MT6885, MT6886, MT6889, MT6890, MT6891, MT6893, MT6895, MT6895T, MT6896, MT6897, MT6980, MT6980D, MT6983, MT6985, MT6989 y MT6990.
- La vulnerabilidad CVE-2024-20083 a todas las versiones de chipsets de la serie: MT6765, MT6768, MT6779, MT6785, MT8321, MT8385, MT8666, MT8667, MT8755, MT8765, MT8766, MT8768, MT8771, MT8775, MT8781, MT8786, MT8788, MT8789, MT8791T, MT8792, MT8795T, MT8796, MT8797 y MT8798.

3. RECOMENDACIÓN:

- Actualizar los productos afectados a la última versión de firmware disponible que aborda estas vulnerabilidades.

Fuente de Información:	• hxxp://corp.mediatek.com/product-security-bulletin/August-2024

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°180	Fecha: 05-08-2024
		Página: 5 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad crítica de autorización incorrecta en Apache OFBiz		
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:

Se ha reportado una vulnerabilidad de severidad **CRÍTICA** de tipo autorización incorrecta en Apache OFBiz. La explotación exitosa de esta vulnerabilidad podría permitir que usuarios no autorizados ejecuten código de representación de pantalla en las instalaciones Apache OFBiz afectadas.

2. DETALLES:

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-38856 de tipo autorización incorrecta en Apache OFBiz, podría permitir que usuarios no autorizados ejecuten código de representación de pantalla en las instalaciones Apache OFBiz afectadas. Esto podría derivar en un acceso no autorizado a información confidencial, manipulación de datos o ejecución de operaciones no deseadas dentro de la aplicación OFBiz.

Vulnerabilidad de autorización incorrecta en Apache OFBiz. Los puntos finales no autenticados podrían permitir la ejecución del código de representación de pantallas si se cumplen algunas condiciones previas (por ejemplo, cuando las definiciones de pantalla no comprueban explícitamente los permisos del usuario porque dependen de la configuración de sus puntos finales).

Los actores de amenazas la están explotando activamente para ejecutar código malicioso en sistemas vulnerables. Se insta a los usuarios a actualizar a la versión 18.12.15 o posterior para mitigar el riesgo de explotación y los posibles impactos posteriores en proveedores externos.

A. Productos afectados:

- Apache OFBiz hasta la versión 18.12.14.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la versión 18.12.15 que aborda esta vulnerabilidad.
- Revisar y aplicar las comprobaciones de autorización adecuadas (en caso no sea posible realizar una actualización inmediata) en todas las definiciones de pantalla, especialmente aquellas a las que se pueda acceder a través de puntos finales no autenticados.
- Implementar controles de acceso y mecanismos de autenticación adicionales para todos los puntos finales.
- Supervisar los registros del sistema para detectar cualquier actividad sospechosa relacionada con la representación de pantallas o intentos de acceso no autorizados.
- Realizar una auditoría de seguridad exhaustiva de la instalación de OFBiz para identificar y abordar cualquier otra vulnerabilidad potencial.

Fuente de Información:	• hxxps://ofbiz.apache.org/security.html • hxxps://securityonline.info/cve-2024-38856-critical-apache-ofbiz-flaw-opens-door-to-unauthorized-code-execution/ • hxxps://blog.sonicwall.com/en-us/2024/08/sonicwall-discovers-second-critical-apache-ofbiz-zero-day-vulnerability/ • hxxps://lists.apache.org/thread/olxxjk6b13sl3wh9cmp0k2dscvp24l7w • hxxps://www.tenable.com/cve/CVE-2024-38856?utm_source=feedly

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°180	Fecha: 05-08-2024
		Página: 5 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de ejecución remota de código en Python setuptools		
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:

Se ha reportado una vulnerabilidad de severidad **ALTA** de tipo inyección de código Python setuptools. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto la ejecución de código arbitrario en el sistema de destino.

2. DETALLES:

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-6345 de tipo inyección de código, podría permitir a un atacante remoto ejecutar código arbitrario en el sistema de destino. La vulnerabilidad existe debido a una validación de entrada incorrecta al procesar la URL en el módulo package_index de pypa/setuptools. Un atacante remoto puede enviar una solicitud especialmente diseñada y ejecutar código arbitrario en el sistema de destino a través de funciones de descarga.

A. Productos afectados:

- setuptools: 50.0.0 - 69.5.1.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.

Fuente de Información:	• hxxp://huntr.com/bounties/d6362117-ad57-4e83-951f-b8141c6e7ca5 • hxxp://github.com/pypa/setuptools/commit/88807c7062788254f654ea8c03427adc859321f0

Índice alfabético