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

197-2024-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

Un ataque de ransomware afecta a la producción de un conocido fabricante de microchips 4
Vulnerabilidad en IBM Maximo Asset Management 5
Vulnerabilidad en Microsoft Edge 6
Vulnerabilidad crítica en TOTOLINK T10 AC1200 7
Índice alfabético 8

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°197	Fecha: 26-08-2024
		Página: 4 de 8

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Un ataque de ransomware afecta a la producción de un conocido fabricante de microchips		
Tipo de Ataque	Ransomware	Abreviatura	Ransomware
Medios de propagación	Correo electrónico, redes sociales, entre otros		
Código de familia	C	Código de Sub familia	C01
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

La compañía Microchip Technology, una empresa manufacturera de chips con sede en EE.UU. que proporciona semiconductores para sistemas integrados y controladores para sistemas industriales habría sufrido un ataque de ransomware que habría impactado en algunas de sus instalaciones de producción.

2. DETALLES:

El fabricante ha admitido que a principios de mes un ataque de ransomware paralizó sus operaciones de fabricación y probablemente también afecte a su producción en el futuro. El incidente se habría originado en su red de TI.

"El 17 de agosto de 2024, Microchip Technology Incorporated detectó actividad potencialmente sospechosa relacionada con sus sistemas de tecnología de la información. Al detectar el problema, la compañía comenzó a tomar medidas para evaluar, contener y remediar la actividad potencialmente no autorizada", señala Microchip Technology en su revelación del ataque.

"El 19 de agosto de 2024, la compañía determinó que una parte no autorizada interrumpió el uso de ciertos servidores y algunas operaciones comerciales. La compañía tomó rápidamente medidas adicionales para abordar el incidente, incluido el aislamiento de los sistemas afectados, el apagado de ciertos sistemas y el inicio de una investigación con la ayuda de asesores externos de ciberseguridad", añade.

La firma reconoce que, como resultado del incidente, algunas de sus instalaciones están operando a "niveles inferiores a los normales" y su capacidad para cumplir con los pedidos se ve afectada.

3. RECOMENDACIONES:

- Practicar una higiene estricta de las contraseñas. Utilizar contraseñas únicas y complejas para todas las cuentas y cambiarlas periódicamente.
- Habilitar la autenticación de dos factores cuando esté disponible.
- No hacer clic en enlaces sospechosos ni descargar archivos adjuntos de fuentes desconocidas.
- Ejecutar la estrategia 3-2-1 de copias de seguridad, que consiste en realizar tres copias de seguridad de los datos, en mínimo dos medios de almacenamiento diferentes, y albergar una de las copias fuera del sitio o en la nube.
- Mantener siempre actualizado los programas, tanto en los dispositivos como en los servidores, para evitar que los atacantes aprovechen las vulnerabilidades y se infiltren en su red.
- Centrar la estrategia de defensa en la detección de movimientos laterales y el bloqueo de actividades fraudulentas de transferencia de datos confidenciales a Internet (fuga de informaciones).
- Procurar la gestión de un plan que incluya detección, investigación y respuesta a amenazas 24/7, ya sea internamente o en asociación con un proveedor especializado de servicios de detección y respuesta gestionadas.

Fuente de Información:	• hxxps://www.escudodigital.com/ciberseguridad/ataque-ransomware-produccion-fabricante-microchips_60154_102.html • hxxps://es.theepochtimes.com/news/kackers-atacan-proveedor-de-microchips-para-la-defensa-de-ee-uu-1304067.html • hxxps://noticiaspuertosantacruz.com.ar/microchip-sufre-ciberataque-que-afecta-operaciones-y-entregas/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°197	Fecha: 26-08-2024 Página: 5 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en IBM Maximo Asset Management		
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 entidad externa XML (XXE) en IBM Maximo Asset Management. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto ver el contenido de un archivo arbitrario en el servidor o realizar un escaneo de red de la infraestructura interna y externa.

2. DETALLES:

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2024-22354 de tipo inyección de entidad externa XML, podría permitir a un atacante remoto obtener acceso a información confidencial.

La vulnerabilidad existe debido a una validación insuficiente de la entrada XML proporcionada por el usuario. Un atacante remoto puede pasar un código XML especialmente diseñado a la aplicación afectada y ver el contenido de archivos arbitrarios en el sistema o iniciar solicitudes a sistemas externos.

La explotación exitosa de la vulnerabilidad puede permitir a un atacante ver el contenido de un archivo arbitrario en el servidor o realizar un escaneo de red de la infraestructura interna y externa.

A. Productos afectados:

- IBM Maximo Asset Management: 7.6.1.2 - 7.6.1.3.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxp://www.ibm.com/support/pages/node/7160615

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°197	Fecha: 26-08-2024 Página: 6 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en Microsoft Edge		
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 corrupción de memoria en Microsoft Edge (basado en HTML). La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto la ejecución de código arbitrario de forma remota.

2. DETALLES:

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2024-38207 de tipo corrupción de memoria, podría permitir a un atacante remoto la ejecución de código arbitrario de forma remota. Este ataque requiere que un usuario haga clic en un enlace para que un atacante inicie la ejecución remota de código de códigos de operación válidos.

La explotación de esta vulnerabilidad requiere la interacción del usuario, lo que significa que un atacante necesitaría que el usuario realice una acción (como visitar un sitio web malicioso) para que la explotación tenga éxito. Este requisito limita la probabilidad de una explotación generalizada y reduce el riesgo general para los datos del usuario

A. Productos afectados:

- Versiones de Microsoft Edge anteriores a 128.0.2739.42.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38207

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°197	Fecha: 26-08-2024 Página: 7 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad crítica en TOTOLINK T10 AC1200		
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 uso de credenciales codificadas en TOTOLINK T10 AC1200. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto obtener acceso no autorizado al sistema afectado mediante credenciales codificadas.

2. DETALLES:

El TOTOLINK T10 es un sistema de Wi-Fi inteligente para el hogar AC1200 de banda dual diseñado para proporcionar una red inalámbrica confiable en áreas más grandes.

La vulnerabilidad de severidad **crítica**, identificada por MITRE como CVE-2024-8162 de tipo uso de credenciales codificadas afecta a una función desconocida en el archivo /squashfs-root/web_cste/cgi-bin/product.ini, que forma parte del componente Telnet Service, podría permitir a un atacante remoto obtener acceso no autorizado al sistema afectado mediante credenciales codificadas. Esto puede provocar un compromiso total de la confidencialidad, integridad y disponibilidad del sistema. Un atacante podría acceder a información confidencial, modificar las configuraciones del sistema o interrumpir los servicios.

A. Productos afectados:

- TOTOLINK T10 AC1200 versión 4.1.8cu.5207.

3. RECOMENDACIONES:

- Actualizar el paquete afectado cuando el proveedor desarrolle la última versión de software disponible destinada a abordar esta vulnerabilidad. Según la última información proporcionada, actualmente no hay ningún parche disponible para esta vulnerabilidad.
- Aislar los dispositivos TOTOLINK T10 AC1200 afectados de la red si es posible.
- Implementar una segmentación estricta de la red para limitar el acceso a estos dispositivos, en caso el aislamiento no sea factible.
- Monitorear cualquier actividad sospechosa o intentos de acceso no autorizado en estos dispositivos.
- Considerar reemplazar los dispositivos afectados con productos alternativos de proveedores con un mejor historial de respuesta de seguridad.
- Deshabilitar el servicio Telnet si es posible y usar métodos de administración alternativos, en caso los dispositivos deben permanecer en uso.
- Implementar fuertes medidas de seguridad perimetral para restringir el acceso remoto a estos dispositivos.
- Verificar regularmente actualizaciones o parches de TOTOLINK y aplicarlos inmediatamente si están disponibles.
- Implementar capas adicionales de autenticación para acceder a estos dispositivos, incluso si no aborda directamente el problema de credenciales codificadas.

Fuente de Información:	• hxxps://www.security-database.com/detail.php?alert=CVE-2024-8162&utm_source=feedly • hxxp://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-8162 • hxxps://github.com/rohitburke/TOTOLINK

Índice alfabético

Explotación de vulnerabilidades conocidas 5, 6, 7
Ransomware 4