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

224-2024-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°224	Fecha: 27-09-2024
		Página: 4 de 8

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	La estafa Microsoft Blocked, que bloquea Windows por completo		
Tipo de Ataque	Phishing	Abreviatur	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Sub familia	G01
Clasificación temática familia	Fraude		

Descripción

1. ANTECEDENTES:

Un nuevo malware está haciendo estragos entre los usuarios. Sustituye la cuenta de Windows por otra llamada Microsoft Blocked.

2. DETALLES:

Al encender el ordenador, algunos usuarios se han encontrado con una pantalla de inicio de Windows, ligeramente distinta. En lugar de su nombre de cuenta, aparece el nombre "Microsoft Blocked", tanto en minúscula como en mayúscula. Al introducir la contraseña o el PIN habitual para entrar en Windows, no funciona. Se trata de un hackeo del ordenador a través de un malware, que tiene una difícil solución.

Este malware habría ingresado al ordenador a través de un enlace en un email o a través de un fichero infectado que se ha descargado de una web. Casi siempre ocurre cuando se descarga juegos o aplicaciones pirateadas. En algunos casos, los usuarios han recibido llamadas de los atacantes haciéndose pasar por soporte técnico de Microsoft, los cuales envían correos electrónicos con enlaces maliciosos. De alguna manera, logran obtener acceso remoto al equipo y modifican la configuración del sistema para crear esta cuenta bloqueada.

Al cambiar la cuenta solo se puede entrar en Windows con la contraseña asociada a esa cuenta de los ciberdelincuentes. Si el usuario intenta recuperar la contraseña por su cuenta, el sistema pide conectar un USB autorizado, algo que no se puede hacer sin acceso de administrador, ya que el registro ha sido cifrado por los hackers.

Normalmente este tipo de estafas van acompañadas de una serie de instrucciones que recibes por email, o en una ventana en Windows que genera el propio malware, en donde te dicen que te darán la contraseña, si les pagas una determinada cantidad de dinero, normalmente en criptomonedas.

3. RECOMENDACIONES:

- Usar una instalación de Linux para restablecer la contraseña y acceder al sistema sin conexión a internet, en caso de que ya se haya sufrido el ataque, para recuperar el control sin pagar. Luego, se debe localizar y eliminar cualquier software de control remoto instalado por los atacantes y cambiar todas las contraseñas guardadas en el dispositivo..
- Evitar abrir archivos adjuntos o enlaces sospechosos en correos electrónicos no solicitados o mensajes de redes sociales.
- Habilitar la autenticación de dos factores cuando esté disponible.
- Implementar el principio del privilegio mínimo para minimizar el impacto potencial ante cualquier intento de ataque.
- Aplicar parches y actualizar periódicamente el software y las aplicaciones a su última versión, así como realizar evaluaciones de vulnerabilidad periódicas.
- Utilizar un software antimalware confiable en sus dispositivos y mantenerlos actualizados.
- Capacitar a su equipo en las mejores prácticas de ciberseguridad y manténgalos informados sobre las últimas amenazas.

Fuente de Información:	• hxxps://computerhoy.com/ciberseguridad/estafa-microsoft-blocked-bloquea-windows-completo-1407689 • hxxps://www.htcmania.com/showthread.php?t=1708663

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°224	Fecha: 27-09-2024 Página: 5 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de denegación de servicio por fragmentación y reensamblaje de IPv4 en el software Cisco IOS XE		
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:

Cisco ha publicado una vulnerabilidad de severidad **ALTA** de tipo errores de gestión de recursos en la implementación del código de reensamblaje de fragmentación IPv4 en el software Cisco IOS XE. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado generar una condición de denegación de servicio (DoS) en un dispositivo afectado.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-20467 de tipo errores de gestión de recursos en la implementación del código de reensamblaje de fragmentación IPv4 en el software Cisco IOS XE, podría permitir que un atacante remoto no autenticado provoque una condición de DoS en un dispositivo afectado.

Esta vulnerabilidad se debe a una gestión inadecuada de los recursos durante el reensamblado de fragmentos. Un atacante podría aprovechar esta vulnerabilidad enviando tamaños específicos de paquetes fragmentados a un dispositivo afectado o a través de una interfaz habilitada para el reensamblado de fragmentación virtual (VFR) en un dispositivo afectado. Una explotación exitosa podría permitir al atacante hacer que el dispositivo se recargue, lo que resultaría en una condición de DoS.

A. Productos afectados:

- Esta vulnerabilidad afecta a los enrutadores de servicios de agregación Cisco ASR serie 1000 y a los enrutadores de banda ancha convergente Cisco cBR-8 si ejecutan el software Cisco IOS XE versión 17.12.1 o 17.12.1a.

3. RECOMENDACIÓN:

- Actualizar los paquetes afectados a la última versión disponible que Cisco ha lanzado para abordar esta vulnerabilidad. No existen soluciones alternativas.

Fuente de Información:	• hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cpp-vfr-dos-nhHKGgO

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°224	Fecha: 27-09-2024
		Página: 6 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en Atemio AM 520 HD Satellite Receiver de Atelmo		
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 publicado una vulnerabilidad de severidad **CRÍTICA** de tipo inyección de comandos del sistema operativo que afecta al receptor de satélite Atemio AM 520 HD de Atelmo. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar comandos del sistema con privilegios elevados.

2. **DETALLES:**

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2024-9166 de tipo inyección de comandos del sistema operativo que afecta al receptor de satélite Atemio AM 520 HD de Atelmo, podría permitir que un atacante no autorizado ejecute comandos del sistema con privilegios elevados. Esta vulnerabilidad se facilita mediante el uso de la consulta 'getcommand' dentro de la aplicación, lo que permite al atacante obtener acceso root.

A. **Productos afectados:**

- Atemio AM 520 HD: TitanNit 2.01 y anteriores.

3. **RECOMENDACIÓN:**

- Cambiar de dispositivo o asumir el riesgo, ya que el proveedor Atelmo ha indicado que este producto ha sido descontinuado. No hay direcciones de servicio o soporte a las que se pueda contactar.

Fuente de Información:	• hxxps://www.cisa.gov/news-events/ics-advisories/icsa-24-270-03 • hxxps://www.atelmo.com/epages/Atelmo.sf/de_DE/?ObjectPath=/Shops/Atelmo/Categories/Service/Kontakt

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°224	Fecha: 27-09-2024 Página: 7 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de ejecución remota de código por inyección de comandos en Lenovo Service Bridge		
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 publicado una vulnerabilidad de severidad **ALTA** de tipo inyección de comandos del sistema operativo en Lenovo Service Bridge. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en el dispositivo afectado.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-4696 de tipo inyección de comandos del sistema operativo, podría permitir a un atacante remoto ejecutar código arbitrario en las instalaciones afectadas de Lenovo Service Bridge. Para explotar esta vulnerabilidad se requiere la interacción del usuario, ya que el objetivo debe visitar una página maliciosa o abrir un archivo malicioso.

La falla específica existe dentro del módulo "LscShim". Al analizar una URL creada, el proceso no valida correctamente una cadena proporcionada por el usuario antes de usarla para ejecutar una llamada al sistema. Un atacante puede aprovechar esta vulnerabilidad para ejecutar código en el contexto del usuario actual.

A. Productos afectados:

- Lenovo Service Bridge, anterior a la versión 5.0.2.17.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps://support.lenovo.com/ca/en/product_security/ps500631-lenovo-service-bridge-vulnerability • hxxps://support.lenovo.com/us/en/product_security/LEN-163429

Índice alfabético