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

103-2024-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°103	Fecha: 03-05-2024
		Página: 4 de 8

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Nueva Botnet “Goldoon” Que Secuestra Enrutadores D-Link Para Utilizarlos En Otros Ataques		
Tipo de Ataque	Botnets	Abreviatura	Botnets
Medios de propagación	IRC, USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C01
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

Los investigadores de seguridad de FortiGuard Labs descubrieron una nueva botnet en abril que explota una debilidad en los dispositivos D-Link.

Esta botnet, denominada "Goldoon", explota una falla de seguridad de casi una década, CVE-2015-2051, para obtener control no autorizado sobre los enrutadores afectados y llevar a cabo actividades maliciosas.

2. DETALLES:

La vulnerabilidad CVE-2015-2051 se encuentra en la interfaz del Protocolo de administración de red doméstica (HNAP) de los dispositivos D-Link. Permite a atacantes remotos ejecutar comandos arbitrarios a través de una acción GetDeviceSettings, que puede manipularse mediante una solicitud HTTP diseñada que contiene un comando malicioso.

Trend Micro dijo que la botnet Goldoon inicia su ataque explotando dicha vulnerabilidad para implementar un script "dropper" desde un servidor malicioso.

Este script está diseñado para borrarse automáticamente para evitar la detección y es capaz de funcionar en varias arquitecturas de sistemas Linux.

Una vez que el dispositivo se ve comprometido, el dropper descarga y ejecuta un archivo, preparando el escenario para futuras actividades maliciosas.

La función principal del dropper es descargar el archivo de la botnet, lo que hace empleando una clave XOR para descifrar cadenas específicas y construir el identificador uniforme de recursos (URI) completo para la carga útil.

Luego, el descargador utiliza un encabezado codificado para recuperar la carga útil final, participando en mecanismos de limpieza para cubrir sus huellas en el sistema comprometido.

Una vez establecido, el malware Goldoon es capaz de lanzar una variedad de ataques distribuidos de denegación de servicio (DDoS), utilizando métodos como inundación TCP, inundación ICMP y ataques más especializados como Minecraft DDoS. Estos ataques pueden afectar tanto a objetivos individuales como a redes más grandes, provocando interrupciones importantes.

3. RECOMENDACIONES:

- Actualizar sus dispositivos D-Link lo antes posible.
- Utilizar herramientas de monitoreo de productos de seguridad para reconocer y bloquear el acceso de los actores de amenazas.
- Habilite la protección de firewall para monitorear y controlar el tráfico de red entrante y saliente.

Fuente de Información:	• hxxps://gbhackers.com/goldoon-botnet-hijacking/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°103	Fecha: 03-05-2024 Página: 5 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades críticas en el sistema de gestión de energía industrial DIAEnergie de Delta Electronics		
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 múltiples vulnerabilidades de severidad **CRÍTICA** de tipo inyección SQL y recorrido de ruta que afecta al sistema de gestión de energía industrial DIAEnergie de Delta Electronics. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante autenticado con privilegios limitados escalar privilegios, recuperar información confidencial, cargar archivos arbitrarios, implementar una puerta trasera a la aplicación y comprometer el sistema en el que se implementa DIAEnergie.

2. DETALLES:

El sistema de gestión de energía industrial DIAEnergie de Delta Electronics permite a las empresas visualizar y mejorar sus sistemas eléctricos y de potencia, especialmente equipos de alto consumo de energía, mediante intervención manual y control de automatización, utilizando adquisición de datos, análisis sistemático, resolución de problemas y diagnóstico de ahorro de energía. El sistema ayuda a monitorear y analizar el consumo de energía en tiempo real, calcular el consumo de energía y las características de carga, optimizar el rendimiento del equipo, mejorar los procesos de producción y maximizar la eficiencia energética.

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-34031 de tipo Inyección SQL, se debe a un error en el script Handler_CFG.ashx. Un atacante autenticado puede aprovechar este problema para comprometer potencialmente el sistema en el que está implementado DIAEnergie.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-34032 de tipo Inyección SQL, se debe a un error en el punto final GetDIACloudList. Un atacante autenticado puede aprovechar este problema para comprometer potencialmente el sistema en el que está implementado DIAEnergie.

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-34033 de tipo Path Traversal, se debe a que Delta Electronics DIAEnergie tiene una validación de entrada insuficiente, lo que permite realizar un ataque de recorrido de ruta y escribir fuera del directorio previsto. Si se especifica un nombre de archivo que ya existe en el sistema de archivos, se sobrescribirá el archivo original.

A. Productos afectados:

- DIAEnergie: Versiones v1.10.00.005.

3. RECOMENDACIÓN:

- Actualizar a DIAEnergie v1.10.01.004 para mitigar estas vulnerabilidades.

Fuente de Información:	• hxxps://www.cisa.gov/news-events/ics-advisories/icsa-24-123-02

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°103		Fecha: 03-05-2024
			Página: 6 de 8
Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Microsoft no solucionará errores "0x80070643" en múltiples versiones de Windows		
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:

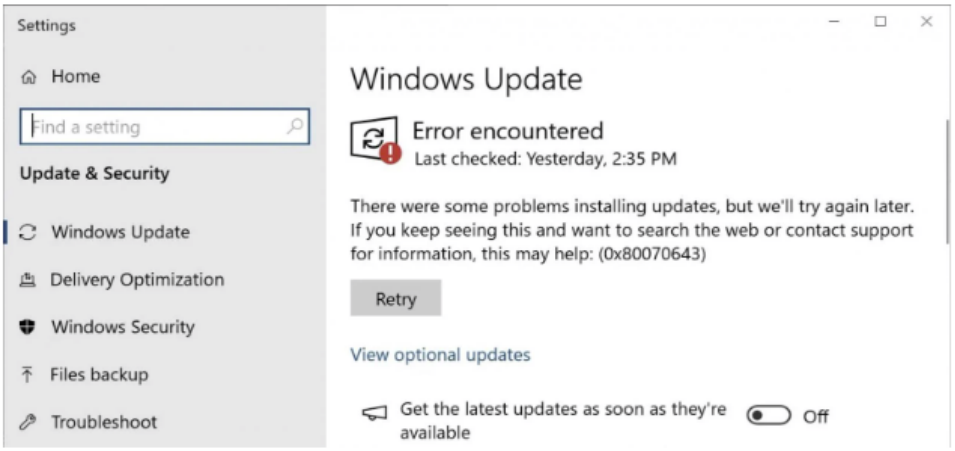
Microsoft ha confirmado que no proporcionará una solución automatizada para un problema conocido que causa errores "0x80070643" al instalar actualizaciones recientes del Entorno de recuperación de Windows (WinRE). La instalación de actualizaciones lanzados en enero de 2024, han generado que equipos con múltiples versiones del sistema operativo de Windows se vean afectados por un error en sistemas con una partición del Entorno de recuperación de Windows (WinRE) demasiada pequeña para que se instale la actualización.

2. DETALLES:

Las actualizaciones problemáticas se publicaron durante el martes de parches de enero de 2024 para corregir la vulnerabilidad de severidad **alta** registrada como CVE-2024-20666 de tipo omisión de la característica de seguridad de BitLocker, podría permitir a un atacante eludir la función de cifrado de dispositivo BitLocker en el dispositivo de almacenamiento del sistema. Un atacante con acceso físico al objetivo podría aprovechar esta vulnerabilidad para obtener acceso a datos cifrados.

El problema afecta al Sistema operativo Windows 10 21H2/22H2 (KB5034441), Windows 11 21H2 (KB5034440) y Windows Server 2022 (KB5034439). Los sistemas afectados, muestran un mensaje de error genérico "0x80070643: ERROR_INSTALL_FAILURE" en lugar del error correcto "CBS_E_INSUFFICIENT_DISK_SPACE" en sistemas con una partición del Entorno de recuperación de Windows (WinRE) demasiada pequeña para que se instale la actualización. Si la partición de recuperación no tiene suficiente espacio libre, se producirá un error en esta actualización.

Microsoft reconoció este problema conocido en enero, días después de informes generalizados de usuarios de Windows sobre errores "0x80070643" y fallas en la instalación de los paquetes de actualización.



Error de actualización de Windows 0x80070643 (BleepingComputer)

Para solucionar los problemas de instalación, Microsoft indicó a sus usuarios afectados que debían expandir su partición WinRE en 250MB de espacio libre para dar una mayor capacidad a la nueva actualización, y ofreció instrucciones detalladas sobre cómo hacerlo. Asimismo, compartió un script de PowerShell para automatizar la instalación de las correcciones de BitLocker después de que WinRE haya cambiado de tamaño correctamente.

El script de PowerShell monta la imagen de WinRE, aplica una actualización dinámica de sistema operativo seguro específica de la arquitectura que debe descargar del catálogo de actualizaciones de Windows antes de ejecutar el script, desmonta la imagen y reconfigura WinRE para el servicio BitLocker si el protector BitLocker TPM está presente.

A. Productos afectados:

- Windows 10 21H2/22H2, Windows 11 21H2 y Windows Server 2022.

3. RECOMENDACIONES:

- Expandir la partición WinRE a 250 MB de espacio libre para dar una mayor capacidad a la nueva actualización y solucionar el problema de instalación. Si la partición de recuperación no tiene suficiente espacio libre, se producirá un error en esta actualización;
- Cambiar el tamaño de las particiones WinRE manualmente, ya que el proveedor no lanzará una solución automatizada para solucionar el problema que causa los errores de instalación de la actualización de Windows "0x80070643". La resolución automática de este problema no estará disponible en una futura actualización de Windows. Son necesarios pasos manuales para completar la instalación de esta actualización en dispositivos que experimentan este error.

Fuente de Información:	• hxxps://www.bleepingcomputer.com/news/microsoft/microsoft-wont-fix-windows-0x80070643-errors-manual-fix-required/ • hxxp://support.microsoft.com/en-us/topic/kb5028997-instructions-to-manually-resize-your-partition-to-install-the-winre-update-400faa27-9343-461c-ada9-24c8229763bf • hxxps://www.bleepingcomputer.com/news/microsoft/microsoft-shares-script-to-update-windows-10-winre-with-bitlocker-fixes/ • hxxps://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20666 • hxxps://learn.microsoft.com/en-us/windows/release-health/status-windows-server-2022#the-january-2024-windows-re-update-might-fail-to-install

Índice alfabético