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

111-2024-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°111	Fecha: 13-05-2024
		Página: 4 de 7

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	El operador móvil chileno WOM expone un millón de contratos de clientes		
Tipo de Ataque	Robo de información	Abreviatura	RobInfo
Medios de propagación	Red, Internet, Redes sociales		
Código de familia	K	Código de Sub familia	K01
Clasificación temática familia	Uso inapropiado de recursos		

Descripción

1. ANTECEDENTES:

WOM, compañía de telecomunicaciones chilena que fue fundada en 2015 después de que el fondo de capital privado Novator Partners adquiriera Nextel Chile, y que cuenta con 8 millones de clientes, ha sufrido una importante brecha de seguridad que ha afectado a gran parte de sus usuarios.

Cabe indicar que en abril la compañía se había declarado en bancarrota.

2. DETALLES:

La empresa había alojado en la nube un directorio llamado 'wom-contratos' que no estaba protegido con ningún tipo de contraseña.

Dicho directorio contenía más de un millón de archivos con contratos móviles de prepago escaneados.

Estos documentos mostraban datos de los clientes, como su nombre completo, número de teléfono, dirección física, dirección de email, fecha y lugar de la firma del contrato y el número de RUT (Rol Único Tributario), un número único establecido en Chile como identificación tributaria.

Lo más preocupante es que todos estos datos fueron accesibles para cualquier persona en Internet durante al menos un par de meses.

El agujero de seguridad ha sido revelado por Cybernews, quien se topó con él a principios de marzo. Sus investigadores descubrieron un bucket S3 de Amazon Web Services (AWS) de acceso público.

Desde Cybernews advierten de que "los números RUT, en combinación con la información de identificación personal (PII), como nombres completos, direcciones y números de teléfono, permiten a los ciberdelincuentes hacerse pasar por personas, abrir cuentas fraudulentas, solicitar crédito o participar en fraudes relacionados con impuestos".

Además, añaden que puede usarse para ataques indiscriminados como phishing y spam, así como para ataques dirigidos, como doxxing y robo de identidad.

En el momento de escribir este artículo la telco chilena no había realizado ningún tipo de comunicación oficial respecto a su agujero de seguridad.

3. RECOMENDACIONES:

- Controlar sus cuentas para detectar cualquier actividad inusual y que tomen precauciones para proteger su información personal.
- Practicar una higiene estricta de contraseñas. Utilizar contraseñas únicas para cada tarjeta y cambiarlas periódicamente.
- Habilitar la autenticación de dos factores cuando esté disponible.
- Mantener el software actualizado. Actualizar periódicamente los sistemas operativos, las aplicaciones y el software de seguridad para corregir las vulnerabilidades.
- Capacitar a los usuarios sobre las mejores prácticas de ciberseguridad.
- Tener cuidado con las estafas telefónicas de soporte técnico que podrían implicar la explotación de los datos robados.

Fuente de Información:	• hxxps://www.escudodigital.com/ciberseguridad/operador-movil-chileno-wom-expone-millon-contratos-clientes_58971_102.html

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°111	Fecha: 13-05-2024
		Página: 5 de 7

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de ejecución remota en CNCSoft-B DOPSoft 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 una vulnerabilidad de severidad **ALTA** de tipo elemento de ruta de búsqueda no controlada que afecta a CNCSoft-B y DOPSoft de Delta Electronics. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto ejecutar código arbitrario en instalaciones afectadas de Delta Electronics CNCSoft-B.

2. DETALLES:

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-1595 de tipo elemento de ruta de búsqueda no controlada que afecta a CNCSoft-B DOPSoft de Delta Electronics. La explotación exitosa de estas vulnerabilidades podría permitir a un Vulnerabilidad de ejecución remota en CNCSoft-B DOPSoft de Delta Electronics atacante remoto ejecutar código arbitrario en instalaciones afectadas de Delta Electronics CNCSoft-B. Se requiere la interacción del usuario para aprovechar esta vulnerabilidad, ya que el objetivo debe visitar una página maliciosa o abrir un archivo malicioso.

La falla específica existe en la carga de imágenes DLL durante el inicio del componente DOPSoft. El proceso no restringe la búsqueda de DLL a rutas confiables, lo que puede resultar en la carga de una DLL maliciosa. Un atacante puede aprovechar esta vulnerabilidad para ejecutar código en el contexto del proceso actual.

A. Productos afectados:

- CNCSoft-B v1.0.0.4.
- DOPSoft: versiones anteriores a v4.0.0.82.

3. RECOMENDACIÓN:

- Actualizar a CNCSoft-B v1.0.0.4, que incluye DOPSoft v4.0.0.94.

Fuente de Información:	• hxxps://www.zerodayinitiative.com/advisories/ZDI-24-441/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°111	Fecha: 13-05-2024 Página: 6 de 7

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades en IBM Storage Fusion HCI		
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 **ALTA** de tipo interpretación inconsistente de las solicitudes HTTP, recorrido del camino y desreferencia del puntero NULO en IBM Storage Fusion HCI. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto no autenticado realizar ataques de phishing, realizar ataques de cruce de directorios y realizar un ataque de denegación de servicio (DoS).

2. DETALLES:

IBM Storage Fusion HCI utiliza aiohttp, criptografía y Gunicorn como parte del servicio de copia de seguridad y restauración y pueden ser vulnerables a los CVE que se enumeran a continuación.

La vulnerabilidad de severidad **media,** identificada por MITRE como CVE-2024-23829 de tipo Interpretación inconsistente de las solicitudes HTTP, podría permitir a un atacante remoto realizar ataques de contrabando de solicitudes HTTP. La vulnerabilidad existe debido a una validación incorrecta de las solicitudes HTTP. Un atacante remoto puede enviar una solicitud HTTP especialmente diseñada al servidor y contrabandear encabezados HTTP arbitrarios. La explotación exitosa de una vulnerabilidad puede permitir a un atacante envenenar la caché HTTP y realizar ataques de phishing.

La vulnerabilidad de severidad **media,** identificada por MITRE como CVE-2024-23334 de tipo recorrido de ruta, podría permitir a un atacante remoto realizar ataques de cruce de directorios. La vulnerabilidad existe debido a un error de validación de entrada al procesar secuencias transversales de directorio en aiohttp.web.static(follow_symlinks=True). Un atacante remoto puede enviar una solicitud HTTP especialmente diseñada y leer archivos arbitrarios en el sistema.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-1135 de tipo interpretación inconsistente de las solicitudes HTTP, podría permitir a un atacante remoto realizar ataques de contrabando de solicitudes HTTP. La vulnerabilidad existe debido a una validación inadecuada de las solicitudes HTTP al manejar encabezados Transfer-Encoding. Un atacante remoto puede enviar una solicitud HTTP especialmente diseñada al servidor y contrabandear encabezados HTTP arbitrarios. La explotación exitosa de una vulnerabilidad puede permitir a un atacante envenenar la caché HTTP y realizar ataques de phishing.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-26130 de tipo desreferencia del puntero NULO, podría permitir a un atacante remoto realizar un ataque de DoS. La vulnerabilidad existe debido a un error de desreferencia de puntero NULL dentro de pkcs12.serialize_key_and_certificates cuando se llama con un certificado y una clave privada que no coinciden y una anulación de hmac_hash. Un atacante remoto puede pasar datos especialmente diseñados a la aplicación y realizar un ataque de DoS.

A. Productos afectados:

- IBM Storage Fusion HCI: anteriores a la versión 2.8.0.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible que aborda estas vulnerabilidades.

Fuente de Información:	• hxxp://www.ibm.com/support/pages/node/7151048 • hxxps://exchange.xforce.ibmcloud.com/vulnerabilities/281079 • hxxps://exchange.xforce.ibmcloud.com/vulnerabilities/281080 • hxxps://exchange.xforce.ibmcloud.com/vulnerabilities/283820 • hxxps://exchange.xforce.ibmcloud.com/vulnerabilities/287833

Índice alfabético