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

Siempre con el pueblo

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Centro Nacional de Seguridad Digital

asbanc
ASOCIACIÓN DE BANCOS DEL PERÚ

Lima, 10 de mayo de 2022

N° 126-2022-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 Aérea del 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 las empresas 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

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 126	Fecha: 10-05-2022
		Página 4 de 8

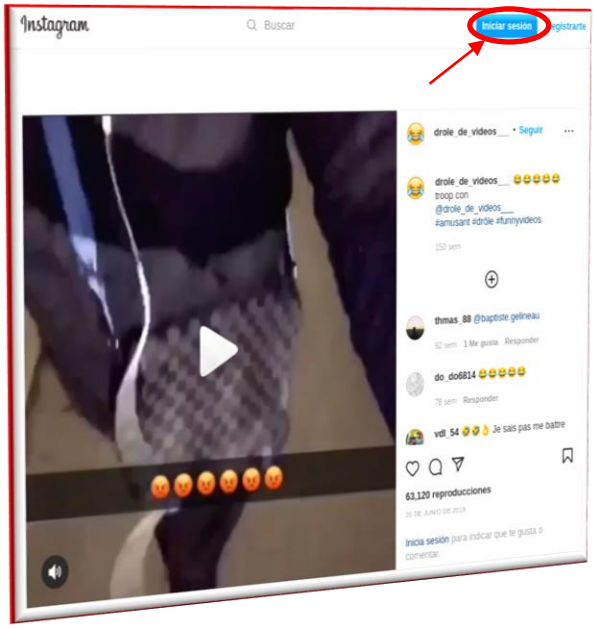
Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Phishing, suplantando la identidad de la red social Instagram		
Tipo de ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de subfamilia	G02
Clasificación temática familia	Fraude		

Descripción

1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes vienen llevando a cabo una campaña de Phishing, donde se viene difundiendo a través de los diferentes navegadores web, quienes suplantan la identidad de la red social Instagram, el cual tiene como finalidad robar información confidencial de las posibles víctimas, como dirección de correo electrónico, número de celular y/o contraseña.

2. Detalles del proceso de estafa del Phishing:

Sitio web falso que suplanta la identidad de Instagram, solicita a la víctima ingresar el usuario (correo electrónico, teléfono o Skype) y contraseña.



Al iniciar sesión, el sitio web falso, le redirige a un video del usuario "drole_de_videos", con la finalidad de aparentar que ha ingresado a su red social de Instagram, sin embargo, las credenciales fueron capturados por los atacantes.

3. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD:**

- **INDICADORES DE COMPROMISO:**

✓ **URL** : hxxps://nospyprod[.]github[.]io/Instagram/

✓ **Dominio** : github.io

✓ **IP** : 185[.]199[.]109[.]153

✓ **SHA-256** : 4eb0407e88a2e12c4424633088deb324315ddfbc68d80b9344dac2a767a9362b

Avira	Suplantación de identidad	CRDF	Malicioso
Emsisoft	Suplantación de identidad	ESET	Suplantación de identidad
Buscador de amenazas de Forcepoint	Suplantación de identidad	Fortinet	Suplantación de identidad
G-datos	Suplantación de identidad	Navegación segura de Google	Suplantación de identidad
kaspersky	Suplantación de identidad	Leonico	Suplantación de identidad

- **OTRAS DETECCIONES:**

4. Referencia:

- Phishing o suplantación de identidad: Es un método que los ciberdelincuentes, utilizan para engañar a los usuarios para conseguir que revele información personal, como contraseñas, datos de tarjetas de créditos, números de cuentas bancarias, entre otros.

5. ALGUNAS RECOMENDACIONES:

- Verificar detalladamente las URL de los sitios web.
- No abrir o descargar archivos sospechosos.
- No seguir las instrucciones del sitio web sospechoso.
- Mantener el antivirus actualizado.

Fuentes de información	▪ Análisis propio de redes sociales y fuente abierta.

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 126	Fecha: 10-05-2022
		Página 6 de 8

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades críticas en productos Schneider Electric		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. Resumen:

Los investigadores McKade Umbenhower y Tony Nasr, han reportado múltiples vulnerabilidades de severidad CRÍTICA y ALTA de tipo uso de credenciales en texto claro, validación de entrada incorrecta, uso de credenciales codificadas, restricción incorrecta de intentos de autenticación excesivos, falta el cifrado de datos confidenciales y transferencia incorrecta de recursos entre esferas en varios productos Schneider Electric. La explotación de estas vulnerabilidades podría permitir a un atacante ejecutar código remoto, provocar una condición de denegación de servicio (DoS) y ejecutar código arbitrario.

2. Detalles:

- La vulnerabilidad de severidad crítica identificada como CVE-2022-30234 de uso de credenciales en texto claro podría permitir la ejecución de código arbitrario cuando se obtiene el nivel de acceso root.
- La vulnerabilidad de severidad alta identificada como CVE-2022-30235 de restricción incorrecta de intentos de autenticación excesivos podría permitir el acceso no autorizado cuando un atacante utiliza la fuerza bruta.
- La vulnerabilidad de severidad alta identificada como CVE-2022-30236 de transferencia incorrecta de recursos entre esferas podría permitir el acceso no autorizado cuando un atacante utiliza ataques entre dominios.
- La vulnerabilidad de severidad alta identificada como CVE-2022-30237 de cifrado faltante de datos confidenciales podría permitir la recuperación de las credenciales de autenticación cuando un atacante rompe la codificación.
- La vulnerabilidad de severidad alta identificada como CVE-2022-30238 de autenticación incorrecta podría permitir que un atacante se haga cargo de la cuenta de administrador cuando un atacante secuestra una sesión.
- La vulnerabilidad de severidad alta identificada como CVE-2022-30232 de validación de entrada incorrecta podría causar una posible ejecución remota de código cuando un atacante puede interceptar y modificar una solicitud en la misma red o tiene acceso de configuración a un dispositivo ION en la red.
- La vulnerabilidad de severidad media identificada como CVE-2022-30233 de validación de entrada incorrecta que podría permitir que el producto sea manipulado maliciosamente cuando se engaña al usuario para que realice ciertas acciones en una página web.
- La vulnerabilidad de severidad media identificada como CVE-2022-6996 en el contexto de Saitel DP RTU, podría conducir a la denegación de servicio cuando un atacante obtiene acceso a la red de comunicación RTU.

3. Productos afectados:

- PowerLogic ION Setup, versiones anteriores a 3.2.22096.01;
- Saitel DP RTU, versiones de firmware desde Baseline_09.00.00 hasta Baseline_11.06.23;
- versiones 4.5 y anteriores de Wiser Smar EER21000 y EER21001.

4. Solución:

- Schneider Electric recomienda actualizar los productos afectados a una versión disponible que corrigen estas vulnerabilidades:
  - Actualizar PowerLogic ION Setup a la versión 3.2.22096.01;
  - Actualizar Saitel DP RTU a la versión de firmware BaseLine_11.06.24;
  - Wiser Smart EER21000 y EER21001 han alcanzado el final de su vida útil (EOL) y no recibirán más soporte, por lo que se recomienda a los usuarios aplicar las medidas listadas en el apartado Mitigations de SEVD-2022-130-03.

Fuentes de información	▪ hxxps://www.se.com/ww/en/download/document/SEVD-2022-130-01/ ▪ hxxps://www.se.com/ww/en/download/document/SEVD-2022-130-02/ ▪ hxxps://www.se.com/ww/en/download/document/SEVD-2022-130-03/

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 126**	**Fecha: 10-05-2022**
		Página 7 de 8

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad crítica de ejecución remota de código en el sistema de archivos de red de Windows Server		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. Resumen:

Microsoft ha reportado una vulnerabilidad de severidad CRÍTICA de tipo validación de entrada incorrecta en el sistema de archivos de red (NFS) de múltiples versiones de Windows Server. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado la ejecución remota de código (RCE) en el sistema vulnerable.

2. Detalles:

- La vulnerabilidad de validación de entrada incorrecta se debe a que el producto afectado recibe entradas o datos, pero no valida o valida incorrectamente que la entrada tiene las propiedades necesarias para procesar los datos de forma segura y correcta.

  La validación de entrada es una técnica de uso frecuente para verificar entradas potencialmente peligrosas a fin de garantizar que las entradas sean seguras para el procesamiento dentro del código o cuando se comuniquen con otros componentes. Cuando el software no valida la entrada correctamente, un atacante puede crear la entrada en una forma que el resto de la aplicación no espera. Esto dará lugar a que partes del sistema reciban entradas no deseadas, lo que puede resultar en un flujo de control alterado, control arbitrario de un recurso o ejecución de código arbitrario.

- La vulnerabilidad identificada como CVE-2022-26937 podría permite que un atacante remoto ejecute código arbitrario en el sistema. La vulnerabilidad existe debido a una validación insuficiente de la entrada proporcionada por el usuario en el sistema de archivos de red de Windows. Un atacante remoto puede pasar una entrada especialmente diseñada a la aplicación y ejecutar código arbitrario en el sistema de destino.

- Esta vulnerabilidad podría explotarse a través de la red al realizar una llamada no autenticada especialmente diseñada a un servicio de Sistema de archivos de red para activar una ejecución remota de código.

3. Productos afectados:

- Windows Server: versión 2008, 2008 R2, 2012, 2012 R2, 2016, 2019, 2019 20H2, 2019 1709, 2019 1803, 2019 1903, 2019 1909, 2019 2004 y 2022.

4. Solución:

Se recomienda instalar las actualizaciones correspondientes desde el sitio web del proveedor. Esta vulnerabilidad no se puede explotar en NFSV4.1. Microsoft señala que antes de actualizar su versión de Windows que protege contra esta vulnerabilidad, puede mitigar un ataque, al deshabilitar NFSV2 y NFSV3. Esto puede afectar negativamente a su ecosistema y sólo debe usarse como una mitigación temporal.

Fuentes de información	▪ hxxps://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-26937

Índice alfabético