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

Lima, 20 de setiembre de 2022

N° 257-2022-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

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 257**	**Fecha: 20-09-2022**
		Página 04 de 08

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades críticas en Switches HPE SAN con Brocade FOS		
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:

Hewlett Packard Enterprise (HPE) ha reportado múltiples vulnerabilidades de severidad CRÍTICA de tipo escritura fuera de los límites, desbordamiento de enteros o ajuste, lectura fuera de los límites, desbordamiento de búfer clásico, restricción incorrecta de operaciones dentro de los límites de un búfer de memoria y desbordamiento de enteros o ajuste en HPE SAN Switches con Brocade Fabric OS (FOS). La explotación exitosa de estas vulnerabilidades podría permitir a un atacante local y remoto ejecutar código de forma arbitraria, causar una denegación de servicio, divulgar o acceder a información sensible, escalar privilegios, causar una corrupción de memoria y realizar accesos no autorizados a archivos.

2. Detalles:

- Estas vulnerabilidades podrían explotarse de forma local o remota para ejecutar código arbitrariamente, provocar la denegación de servicio, realizar la divulgación de información confidencial, obtener privilegios elevados, acceder a información confidencial, causar daños en la memoria y realizar acceso no autorizado a archivos.
- Las vulnerabilidades críticas han sido identificadas como: CVE-2014-9984, CVE-2015-4042, CVE-2017-16548, CVE-2018-6485, CVE-2019-9169, CVE-2021-3711 y CVE-2021-39275.

3. Productos afectados:

Los Switches HPE SAN con las siguientes versiones de Brocade Fabric OS (FOS) son vulnerables:

- Brocade Fabric OS (FOS) versión, 9.1 anteriores a 9.1.1;
- Brocade Fabric OS (FOS) versión, 9.0 anteriores a 9.0.1e;
- Brocade Fabric OS (FOS) versión, 8.2 anteriores a 8.2.3c;
- Brocade Fabric OS (FOS) versión, 7.4 anteriores a 7.4.2j.

4. Solución:

HPE recomienda actualizar los productos afectados con la última versión de firmware disponible que corrigen estas vulnerabilidades:

- Firmware FOS de la versión 9.1.1 o posterior para los Switches de canal de fibra de la serie B de HPE;
- Firmware FOS versión 9.0.1e o posterior para Switches de canal de fibra HPE serie B;
- Firmware FOS versión 8.2.3c o posterior para Switches de canal de fibra HPE serie B;
- Firmware FOS de la versión 7.4.2j o posterior para los Switches de canal de fibra de la serie B de HPE.

Fuentes de información	▪ hxxps://www.incibe-cert.es/alerta-temprana/avisos-seguridad/multiples-vulnerabilidades-hpe-san-switches-brocade-fos ▪ hxxps://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbst04367en_us

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 257**	**Fecha: 20-09-2022**
		Página 05 de 08

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad crítica en el sistema de planificación energética PROMOD IV de Hitachi Energy		
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:

Se ha reportado una vulnerabilidad de severidad CRÍTICA de tipo control de acceso inadecuado en el sistema de planificación energética PROMOD IV de Hitachi Energy. La explotación exitosa de esta vulnerabilidad podría permitir que un atacante remoto eliminar archivos arbitrarios una vez que el sistema esté comprometido.

2. Detalles:

- La vulnerabilidad de severidad **crítica** identificada como CVE-2010-3591 de control de acceso inadecuado en el módulo Actbar2.ocx incluido en los productos afectados, podría permitir a un atacante remoto eliminar datos del sistema local o modificar el flujo de trabajo, lo que podría afectar la forma en que el sistema de energía interpreta y responde a las entradas.
- La vulnerabilidad de tipo control de acceso inadecuado se debe a que el software no restringe o restringe incorrectamente el acceso a un recurso de un actor no autorizado.

3. Productos afectados:

Las siguientes versiones del PROMOD IV y del PROMOD-Generador, un sistema de planificación energética, congestión de transmisión y previsión de precios se ven afectadas:

- Hitachi Energy PROMOD IV Versión: 11.2, 11.3 y 11.4.

4. Solución:

- Hitachi Energy señala que está desarrollando PROMOD IV a la versión 11.5, que contendrá un parche que corregirá esta vulnerabilidad. Asimismo, indicaron que PROMOD IV ya no utiliza Actbar2.ocx. Se recomienda eliminar Actbar2.ocx.
- Hitachi Energy recomienda aplicar las siguientes prácticas de seguridad y configuraciones de firewall para ayudar a proteger una red de control de procesos de ataques que se originan desde fuera de la red:
  - Proteger físicamente los sistemas de control de procesos del acceso directo no autorizado;
  - Separar los sistemas de control de procesos de otras redes utilizando un sistema de firewall con la cantidad mínima de puertos abiertos;
  - Los sistemas de control de procesos no deben utilizarse para navegar por Internet, enviar mensajes instantáneos o recibir correos electrónicos;
  - PROMOD IV debe implementarse dentro de la red de la zona desmilitarizada (DMZ) de la empresa;
  - Las computadoras portátiles y los medios de almacenamiento extraíbles deben escanearse cuidadosamente en busca de virus antes de conectarse a un sistema de control;
  - Los usuarios deben seguir las pautas de refuerzo publicadas por The Center for Internet Security (CIS) para proteger el sistema operativo host.

Fuentes de información	▪ hxxps://www.cisa.gov/uscert/ics/advisories/icsa-22-263-01

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 257	Fecha: 20-09-2022
		Página 06 de 08

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Phishing, suplantado la identidad del sitio web del Banco Interbank.		
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 se vienen llevando a cabo una campaña de Phishing, a través de los diferentes navegadores web, vienen suplantando el sitio oficial del Banco Interbank (Banca por internet), con el objetivo de acceder u obtener datos personales y/o bancarios vinculado a la cuenta.

2. Detalles del proceso de Phishing:

Imagen 1: Solicita a las víctimas que ingrese las credenciales de acceso (N° de tarjeta, DNI y clave web).

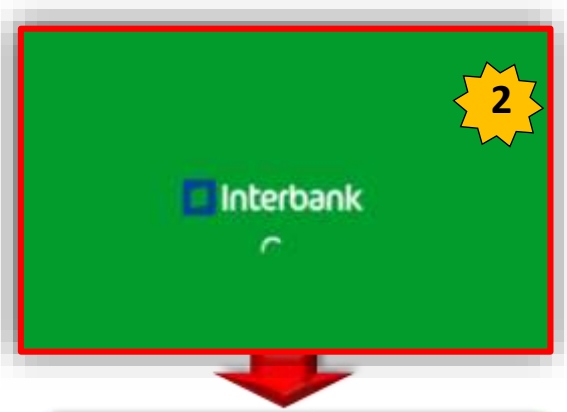


Imagen 2: Una vez ingresado los datos solicitados, muestra una ventana aparentemente de la entidad financiera Interbank, aludiendo como si estuviese cargando dicha página.

3. Comparación del sitio web oficial del Banco Interbank con el fraudulento:

SITIO WEB OFICIAL

URL: https://bancaporintenet.interbank.pe/login

SITIO WEB FRAUDULENTO

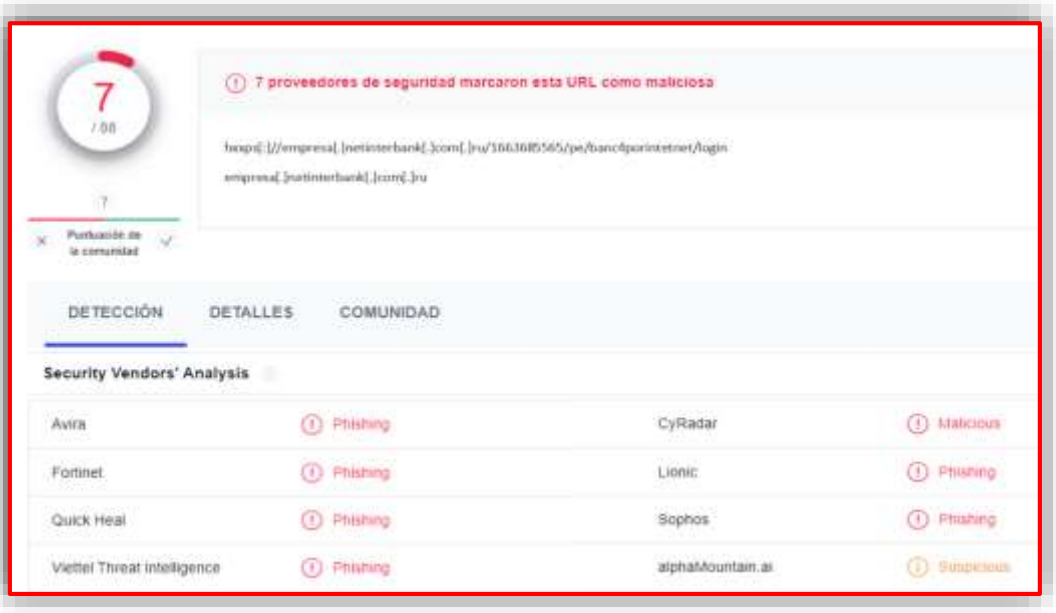
URL: hxxps[:]//empresa[.]netinterbank[.]com[.]ru/1663685565/pe/banca/porintetnet/login

- Existe similitud entre ambas páginas, en imagen, fondo y escritura la diferencia se encuentra en la URL.
- La URL falsa utiliza protocolo HTTPS, no significa que la web sea segura.
- El dominio (empresa.netinterbank.com.ru) del sitio web fraudulento se encuentra reportado como **PHISHING.**
- La URL falsa está mal escrita y los caracteres ambiguos

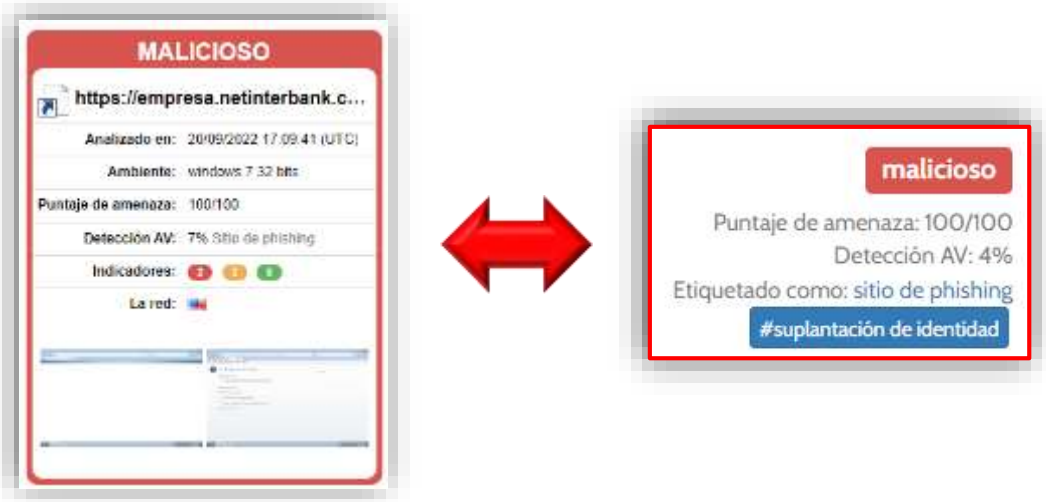
4. **La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como SUPLANTACIÓN DE IDENTIDAD – PHISHING:**

- **INDICADORES DE COMPROMISO:**

  - ✓ **URL:** hxxps[:]//empresa[.]netinterbank[.]com[.]ru/1663685565/pe/banc4porintetnet/login
  - ✓ **Dominio:** empresa.netinterbank.com.ru
  - ✓ **IP:** 104[.]21[.]87[.]31
  - ✓ **Código:** 404



- **OTRAS DETECCIONES:**



5. **Algunas Recomendaciones:**

- Verificar la información en la entidad correspondiente.
- Acceder al sitio web a través de fuentes oficiales.
- No abrir enlaces de dudosa procedencia.
- No seguir indicaciones de sitios web fraudulentos.
- No compartir la información con terceras personas, amigos o familiares.
- Mantener instalado un servicio de antivirus en el dispositivo.

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

Índice alfabético