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, 16 de setiembre de 2022

N° 253-2022-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

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 253	Fecha: 16-09-2022
		Página 04 de 11

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Hackeo de UBER		
Tipo de ataque	Robo de información	Abreviatura	Robinfo
Medios de propagación	Red, Internet		
Código de familia	K	Código de subfamilia	K01
Clasificación temática familia	Uso inapropiado de recursos		

Descripción

Segu Info reveló en setiembre, que Uber ha sido hackeado, los sistemas internos y documentos confidenciales presuntamente se encuentran comprometidos.

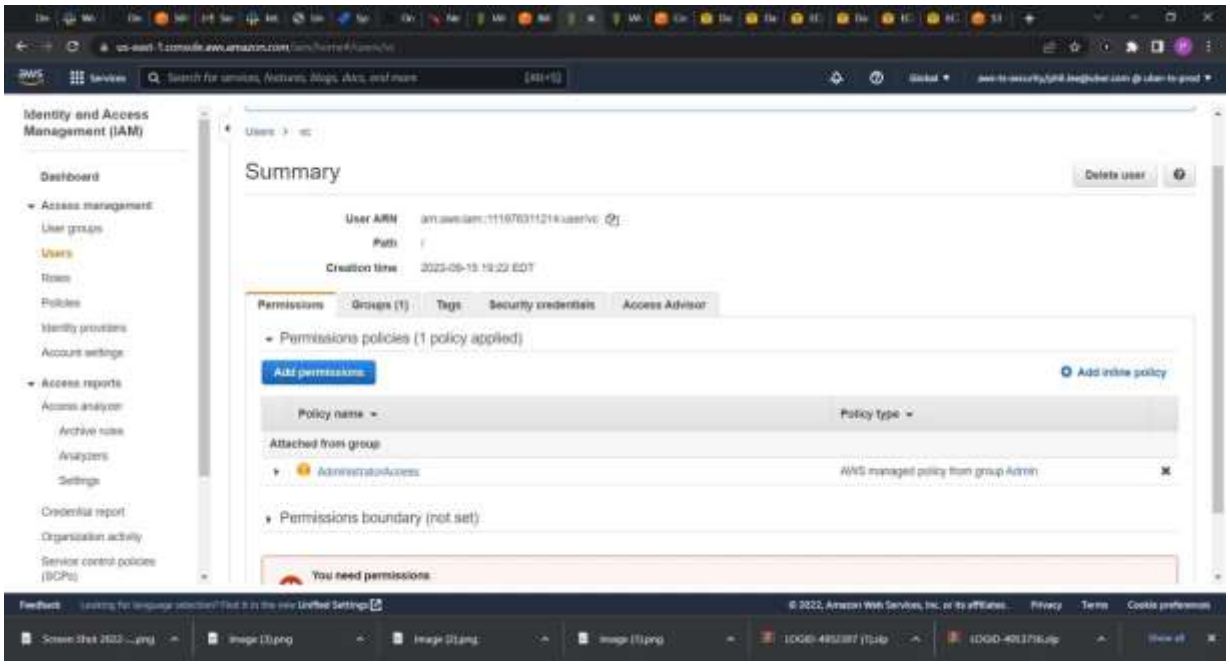
ANTECEDENTES:

- Esta no es la primera vez que la empresa sufre una brecha de seguridad. En 2017, la noticia de otra filtración de datos que tuvo lugar en 2016 fue noticia.
- En noviembre de 2017, el CEO de Uber, Dara Khosrowshahi, anunció que los delincuentes informáticos irrumpieron en la base de datos de la empresa y accedieron a los datos personales (nombres, direcciones de correo electrónico y números de teléfono celular) de 57 millones de sus usuarios, la revelación desconcertante fue que la empresa encubrió el hackeo durante más de un año.
- Los atacantes accedieron también a los nombres y números de licencia de conducir de aproximadamente 600.000 de sus conductores en los Estados Unidos.
- El hackeo ocurrió en 2016, fue fácil para los atacantes que, según un informe publicado por Bloomberg, obtuvieron credenciales de un sitio privado de GitHub utilizado por el equipo de desarrollo de la empresa. Los delincuentes informáticos intentaron chantajear a Uber y exigieron 100.000 dólares a la empresa a cambio de evitar la publicación de los datos robados. En lugar de notificar la violación de datos a los clientes y a las fuerzas del orden, como exige la ley de notificación de violaciones de seguridad de datos de California, el jefe de seguridad de la información, Joe Sullivan, ordenó pagar el rescate y cubrir la historia destruyendo cualquier evidencia. El pago se disfrazó como un premio de recompensa por errores completo con acuerdos de confidencialidad firmados.

DETALLES:

- La fuente del New York Times, reportó que los atacantes hackearon la cuenta de Slack de un empleado y la usaron para informar al personal interno que **"la empresa había sufrido una violación de datos"** y proporcionaron una lista de bases de datos internas presuntamente hackeadas.
- El mensaje decía lo siguiente **"Anuncio que soy un hacker y Uber ha sufrido una violación de datos".**
- La empresa se vio obligada a desconectar sus sistemas internos de comunicaciones e ingeniería para mitigar el ataque e investigar la intrusión, ya que los atacantes supuestamente comprometieron varios sistemas internos y proporcionaron imágenes de correo electrónico, almacenamiento en la nube y repositorios de códigos a The New York Times y algunos investigadores de seguridad cibernética.
- San Curry, ingeniero de seguridad de Yuga Labs, quien mantuvo correspondencia con la persona que afirmó ser responsable de la violación dijo "Prácticamente tienen acceso completo a Uber", "Este es un compromiso total, por lo que parece".
- Asimismo, los atacantes también tenían acceso al programa de recompensas de HackerOne de la empresa, lo que significa que tenían acceso a todos los informes de errores enviados a investigadores de seguridad y esta información es muy importante porque los actores de amenazas podrían usarla para lanzar más ataques. En este momento no es posible descartar que los informes incluyan detalles técnicos sobre algunas fallas que aún no han sido reparadas por la empresa. Por otro lado, HackerOne ha deshabilitado inmediatamente el programa de recompensas por errores de Uber bloqueando cualquier acceso a la lista de problemas informados.

- En la siguiente imagen el atacante afirma haber comprometido completamente a Uber: publicó capturas de pantalla de su instancia de AWS, GCP, el panel de administración de HackerOne y más.



- Latha Maripuri, directora de seguridad de la información de Uber, manifestó a NYT por correo electrónico "No tenemos una estimación en este momento de cuándo se restablecerá el acceso completo a las herramientas, así que gracias por su paciencia".

RECOMENDACIONES:

- Se debe reforzar con estrictos controles de seguridad.
- Se debe utilizar el doble factor de autenticación.
- Implementar seguridad de aplicaciones en tiempo real.

Fuentes de información	▪ hxxps://blog.segu-info.com.ar/2022/09/uber-hackeado-sistemas-internos-y.html ▪ Análisis propio de fuentes abiertas.

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 253**	**Fecha: 16-09-2022**
		Página 06 de 11

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad de denegación de servicio en OpenSSL que afecta a productos industriales de Siemens		
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:

Siemens ha reportado una vulnerabilidad de severidad ALTA de tipo bucle con condición de salida inalcanzable (bucle infinito) en varios de sus productos que usan una versión vulnerable de OpenSSL. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante generar una condición de denegación de servicio (DoS) al proporcionar certificados de curva elíptica especialmente diseñados para productos que usan una versión vulnerable de OpenSSL.

2. Detalles:

- La vulnerabilidad de severidad **alta** identificada como CVE-2022-0778 de bucle infinito en la función **BN_mod_sqrt()** en OpenSSL, que calcula una raíz cuadrada modular, contiene un error que puede hacer que se repita indefinidamente para módulos no primos. Internamente, esta función se usa cuando se analizan certificados que contienen claves públicas de curva elíptica en forma comprimida o parámetros de curva elíptica explícitos con un punto base codificado en forma comprimida. Es posible activar el bucle infinito creando un certificado que tenga parámetros de curva explícitos no válidos. Dado que el análisis del certificado ocurre antes de la verificación de la firma del certificado, cualquier proceso que analice un certificado proporcionado externamente puede estar sujeto a un ataque de denegación de servicio. El bucle infinito también se puede alcanzar al analizar claves privadas diseñadas, ya que pueden contener parámetros de curva elíptica explícitos.
- La vulnerabilidad de tipo bucle infinito se debe a que el programa contiene una iteración o bucle con una condición de salida que no se puede alcanzar, es decir, un bucle infinito.

3. Productos afectados:

- OpenSSL, versiones 1.0.2, 1.1.0, 1.1.1 y 3.0;
- Industrial Edge - Conector OPC UA, todas las versiones anteriores a 1.7;
- Industrial Edge - Aplicación SIMATIC S7 Connector, todas las versiones anteriores a 1.7;
- RUGGEDCOM CROSSBOW Station Access Controller (SAC), todas las versiones solo cuando se ejecutan en ROX II anteriores a 2.15.1;
- RUGGEDCOM RM1224 LTE(4G) UE (6GK6108-4AM00-2BA2), todas las versiones;
- RUGGEDCOM RM1224 LTE(4G) NAM (6GK6108-4AM00-2DA2), todas las versiones;
- RUGGEDCOM ROX MX5000, todas las versiones anteriores a 2.15.1;
- Lista completa aquí.

4. Solución:

- Siemens ha publicado actualizaciones para varios de sus productos afectados y recomienda actualizar los productos afectados a las últimas versiones disponibles que corrigen esta vulnerabilidad. También recomienda aplicar contramedidas para productos donde las actualizaciones no están aún disponibles;

- Asimismo, como medida de seguridad general, Siemens recomienda encarecidamente proteger el acceso a la red a los dispositivos con los mecanismos adecuados. Para operar los dispositivos en un entorno de TI protegido, Siemens recomienda configurar el entorno de acuerdo con las pautas operativas de Siemens para la seguridad industrial, y seguir las recomendaciones de los manuales de los productos;

- OpenSSL versión 1.0.2 está fuera de soporte y ya no recibe actualizaciones públicas (solo está disponible para clientes de soporte Premium), OpenSSL versión 1.1.0 está fuera de soporte y ya no recibe actualizaciones de ningún tipo, se ve afectado por esta vulnerabilidad, se recomienda actualizar a OpenSSL versión 3.0 o 1.1.1n.

Fuentes de información	▪ hxxps://cert-portal.siemens.com/productcert/html/ssa-712929.html ▪ hxxps://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0778 ▪ hxxps://www.openssl.org/news/secadv/20220315.txt

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 253**	**Fecha: 16-09-2022**
		Página 08 de 11

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad en el Agente Cortex XDR de Palo Alto Networks		
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:

Diego García de INCIDE, ha reportado una vulnerabilidad de severidad MEDIA de tipo resolución de enlace incorrecta antes del acceso al archivo (seguimiento del enlace) al generar un archivo de soporte técnico en el **Agente Cortex XDR** de Palo Alto Networks. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante local provocar una violación de la privacidad de los datos, al leer archivos en el sistema con privilegios elevados al generar un archivo de soporte técnico.

2. Detalles:

- La vulnerabilidad de severidad **media** identificada como CVE-2022-0029 de resolución de enlace incorrecta en el agente Cortex XDR de Palo Alto Networks en dispositivos Windows permite que un atacante local lea archivos en el sistema con privilegios elevados al generar un archivo de soporte técnico.
- La vulnerabilidad de tipo seguimiento del enlace se debe a que el software intenta acceder a un archivo en función del nombre de archivo, pero no evita correctamente que ese nombre de archivo identifique un enlace o acceso directo que se resuelva en un recurso no deseado.

3. Productos afectados:

- Agente Cortex XDR, versión 7.5.x CE y anteriores a 7.5.101-CE en Windows;
- Agente Cortex XDR, versión 7.7.x y anteriores a 7.7.3 en Windows;
- Agente Cortex XDR, versión 5.0.x y anteriores a 5.0.12-hotfix en Windows.

4. Solución:

- Palo Alto Networks indicó que esta vulnerabilidad se solucionó en la actualización de revisión del Agente Cortex XDR 5.0.12, el agente Cortex XDR 7.5.101-CE, el agente Cortex XDR 7.7.3 y todas las versiones posteriores del agente Cortex XDR.

Fuentes de información	▪ hxxps://security.paloaltonetworks.com/CVE-2022-0029 ▪ hxxp://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0029

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 253	Fecha: 16-09-2022
		Página 09 de 11

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Phishing, suplantado la identidad del sitio web “Banca por Internet” del Banco de Crédito del Perú (BCP).		
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 financiero		

Descripción

1. A través A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes vienen llevando a cabo una campaña de Phishing, a través de los diferentes navegadores web, quienes vienen suplantando la identidad del sitio web “Banca por Internet” del Banco de Crédito del Perú (BCP), el cual tiene como finalidad robar información confidencial y bancaria de las posibles víctimas como número de tarjeta, clave de internet, token.

2. Detalles del proceso de Phishing:

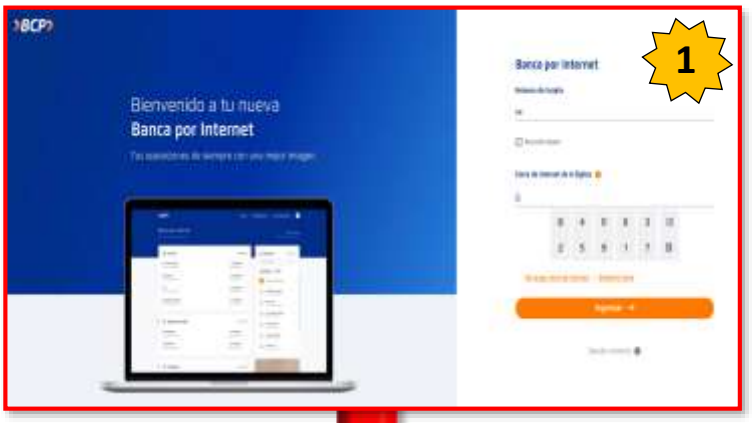


Imagen 1:

Solicita datos bancarios como número de tarjeta y clave bancaria.

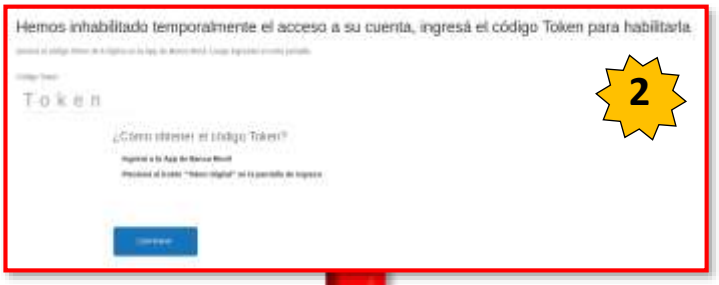


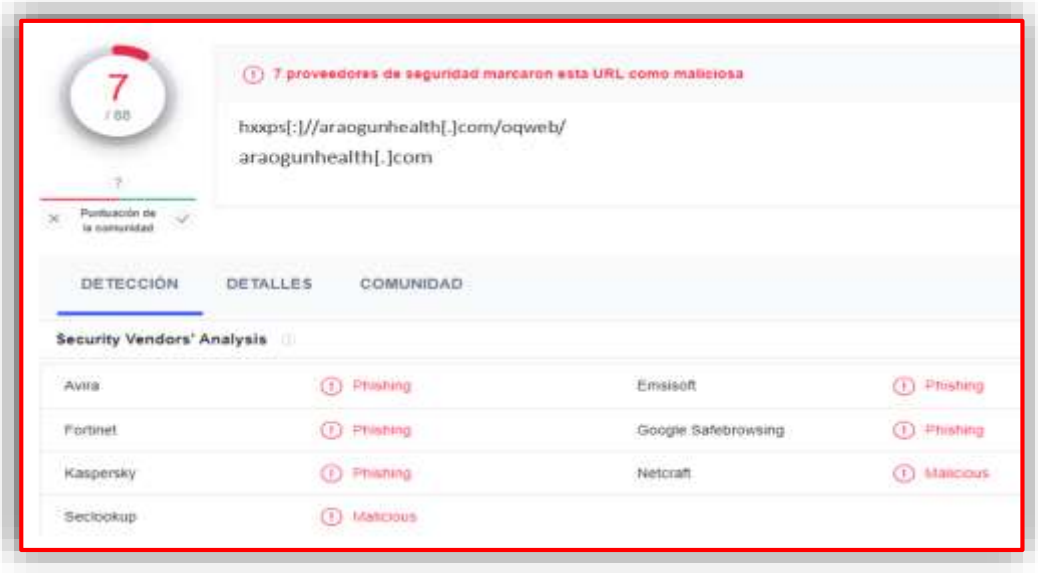
Imagen 2:

Redirige a una ventana en la que se solicita introducir el “Token”, luego vuelve a redirigir a la misma página (Imagen 1).

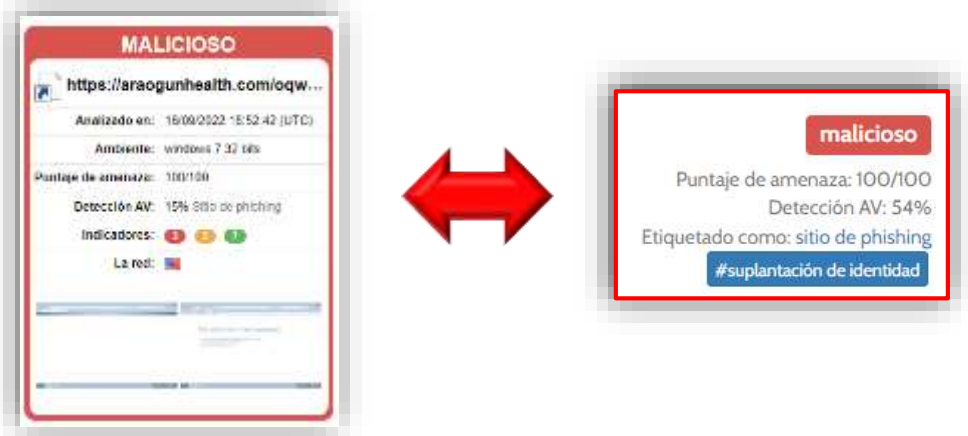
3. **La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como SUPLANTACIÓN DE IDENTIDAD – PHISHING:**

- **INDICADORES DE COMPROMISO:**

  - ✓ **URL:** hxxps[:]//araogunhealth[.]com/oqweb/
  - ✓ **Dominio:** araogunhealth[.]com
  - ✓ **IP:** 216[.]158[.]231[.]179
  - ✓ **Código:** 200
  - ✓ **Longitud:** 59.17 KB
  - ✓ **SHA-256**: 05e844db09f961eada7e431b31c8c5d64e147877db4d93a5a13e5765348da005



- **OTRAS DETECCIONES:**



4. **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