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, 17 de noviembre de 2022

312-2022-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° 312	Fecha: 17-11-2022
		Página 4 de 12

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Actualizaciones de Microsoft de noviembre generan problemas en Kerberos		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de Intrusión		

Descripción

Microsoft está investigando un nuevo problema que hace que los controladores de dominio empresarial experimenten fallas de inicio de sesión de Kerberos y otros problemas de autenticación, después de instalar actualizaciones acumulativas lanzadas durante el martes de parches de este mes.

ANTECEDENTES:

- En los parches de noviembre se corrigieron 68 fallas en total, incluyendo 6 vulnerabilidades de Windows explotadas activamente. Once de las 68 vulnerabilidades se clasificaron como «Críticas», ya que permiten la elevación de privilegios, la suplantación de identidad o la ejecución remota de código.

  - 27 Vulnerabilidades de elevación de privilegios.
  - 04 Vulnerabilidades de omisión de funciones de seguridad.
  - 16 Vulnerabilidades de ejecución remota de código.
  - 11 Vulnerabilidades de divulgación de información.
  - 06 Vulnerabilidades de denegación de servicio.
  - 03 Vulnerabilidades de suplantación de identidad.

DETALLES:

- Los lectores de BleepingComputer también informaron hace tres días que las actualizaciones de noviembre «rompen Kerberos en situaciones en las que ha establecido las opciones de cuenta 'Esta cuenta admite el cifrado Kerberos AES de 256 bits' o 'Esta cuenta admite el cifrado Kerberos AES de 128 bits' (es decir, msDS-atributo SupportedEncryptionTypes) en cuentas de usuario en AD».
- El problema, investigado activamente por Redmond, puede afectar cualquier escenario de autenticación Kerberos dentro de los entornos empresariales afectados. «Después de instalar las actualizaciones lanzadas el 8 de noviembre de 2022 o más tarde en los servidores de Windows con la función de controlador de dominio, es posible que tenga problemas con la autenticación de Kerberos», explicó Microsoft. «Cuando se encuentra este problema, es posible que reciba un evento de error de Microsoft-Windows-Kerberos-Key-Distribution-Center Event ID 14 en la sección Sistema del registro de eventos en su controlador de dominio». Los errores registrados en los registros de eventos del sistema se etiquetarán con la frase «the missing key has an ID of 1».
- La lista de escenarios de autenticación de Kerberos incluye, entre otros, los siguientes:
  - El inicio de sesión del usuario del dominio puede fallar. Esto también podría afectar la autenticación de los Servicios de federación de Active Directory (AD FS).
  - Las cuentas de servicio administradas de grupo (gMSA) utilizadas para servicios como Internet Information Services (IIS Web Server) pueden fallar en la autenticación.
  - Es posible que las conexiones de escritorio remoto que usan usuarios de dominio no se conecten.
  - Es posible que no pueda acceder a carpetas compartidas en estaciones de trabajo y recursos compartidos en servidores.
  - La impresión que requiere autenticación de usuario de dominio puede fallar.

- Este error afecta a las plataformas cliente y servidor:
  - **Cliente:** Windows 7 SP1, Windows 8.1, Windows 10 Enterprise LTSC 2019, Windows 10 Enterprise LTSC 2016, Windows 10 Enterprise 2015 LTSB, Windows 10 20H2 o posterior y Windows 11 21H2 o posterior.
  - **Servidor:** Windows Server 2008 SP2 o posterior, incluida la versión más reciente, Windows Server 2022.

- El problema no afecta a los clientes domésticos y los que no están en un dominio local. Además, no afecta a los entornos híbridos de Azure Active Directory ni a aquellos que no tienen servidores de Active Directory locales.

RECOMENDACIONES:

- Estar atento a las nuevas actualizaciones del sistema operativo de Microsoft (Cliente y Servidor) e instalarlo para solucionar las fallas de inicio de sesión.

Fuentes de información	▪ hxxps://www.bleepingcomputer.com/news/microsoft/windows-kerberos-authentication-breaks-after-november-updates/ ▪ hxxps://blog.segu-info.com.ar/2022/11/actualizaciones-de-microsoft-de.html?m=1 ▪ hxxps://mspoweruser.com/es/kerberos-authentication-issues-due-to-november-updates/ ▪ Análisis propio de redes sociales y fuente abierta

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 312**	**Fecha: 17-11-2022**
		Página 6 de 12

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades en productos de Cisco		
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:**

Cisco ha reportado múltiples vulnerabilidades de severidad ALTA de tipo uso incorrecto de API privilegiadas, inyección de comando de sistema operativo y Cross-site Scripting (XSS) en Cisco Identity Services Engine (ISE). La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto autenticado inyectar comandos arbitrarios del sistema operativo, eludir las protecciones de seguridad y realizar ataques de secuencias de comandos entre sitios.

2. **Detalles:**

- La vulnerabilidad de severidad **alta** identificada como CVE-2022-20964 en la interfaz de administración basada en web de Cisco ISE podría permitir a un atacante remoto autenticado inyectar comandos arbitrarios en el sistema operativo subyacente. Esta vulnerabilidad se debe a la validación incorrecta de la entrada del usuario dentro de las solicitudes como parte de la función tcpdump de la interfaz de administración basada en web. Un atacante con privilegios suficientes para acceder a la función tcpdump podría aprovechar esta vulnerabilidad al manipular las solicitudes a la interfaz de administración basada en web para que contenga los comandos del sistema operativo.

- La vulnerabilidad de severidad **media** identificada como CVE-2022-20965 en la interfaz de administración basada en web de Cisco ISE podría permitir a un atacante remoto autenticado eludir las restricciones de seguridad dentro de la interfaz de administración basada en web. Esta vulnerabilidad se debe a un control de acceso inadecuado en una función dentro de la interfaz de administración basada en web del sistema afectado.

- La vulnerabilidad de severidad **media** identificada como CVE-2022-20966 en la interfaz de administración basada en web de Cisco ISE podría permitir a un atacante remoto autenticado realizar ataques de secuencias de comandos entre sitios contra otros usuarios de la interfaz de administración basada en web de la aplicación. Esta vulnerabilidad se debe a una validación incorrecta de la entrada a una función de la aplicación antes del almacenamiento dentro de la función tcpdump de la interfaz de administración basada en web.

- La vulnerabilidad de severidad **media** identificada como CVE-2022-20967 en la interfaz de administración basada en la web La característica del servidor RADIUS externo de Cisco ISE podría permitir a un atacante remoto autenticado realizar ataques de secuencias de comandos entre sitios contra otros usuarios de la interfaz de administración basada en la web de la aplicación. Esta vulnerabilidad se debe a una validación incorrecta de la entrada a una función de la aplicación antes del almacenamiento dentro de la función del servidor RADIUS externo de la interfaz de administración basada en web.

- Las vulnerabilidades no dependen unas de otras. No se requiere la explotación de una de las vulnerabilidades para explotar otra vulnerabilidad. Además, es posible que una versión de software que se vea afectada por una de las vulnerabilidades no se vea afectada por las otras vulnerabilidades. Estas vulnerabilidades solo pueden ser explotadas por usuarios válidos y autorizados del sistema Cisco ISE. Como práctica recomendada, los clientes pueden restringir el acceso a la consola y el acceso web del administrador.

3. **Productos afectados:**

- Cisco Identity Services Engine, version 2.7, 3.0, 3.1 y 3.2.

4. **Solución:**

- Se recomienda actualizar los productos afectados con las últimas versiones de software disponible.

Fuentes de información	▪ hxxps://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-7Q4TNYUx

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 312**	**Fecha: 17-11-2022**
		Página 8 de 12

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad de desbordamiento de búfer en las bibliotecas Kerberos de Samba		
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 ALTA de tipo desbordamientos de búfer en las bibliotecas Kerberos de Samba en sistemas de 32 bits. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto la ejecución remota de código arbitrario, la denegación remota de servicio y la omisión de políticas de seguridad.

2. **Detalles:**

   - Samba es un componente importante para integrar servidores y escritorios Linux/Unix en entornos de Active Directory (AD). Puede funcionar como controlador de dominio (DC) o como miembro de dominio regular. Samba brinda servicios de archivo e impresión seguros, estables y rápidos para todos los clientes que utilizan el protocolo SMB/CIFS, como todas las versiones de DOS y Windows, OS/2, Linux y muchos otros.

   - La vulnerabilidad de severidad **alta** identificada como CVE-2022-42898 en las bibliotecas Kerberos de Samba y AD DC no pudieron proteger contra el desbordamiento de enteros al analizar un certificado de atributos de privilegio (PAC) en un sistema de 32 bits, lo que permitió a un atacante con un PAC falsificado corromper el montón.

   - Las bibliotecas Kerberos utilizadas por Samba proporcionan un mecanismo para autenticar un usuario o servicio mediante tickets que pueden contener certificados de atributos de privilegio.

   - Tanto las bibliotecas Kerberos de Heimdal como las de MIT, por lo que el Heimdal incorporado enviado por Samba sufren de un desbordamiento de multiplicación de enteros al calcular cuántos bytes asignar para un búfer para el PAC analizado.

   - En un sistema de 32 bits, un desbordamiento permite la colocación de fragmentos de 16 bytes de datos totalmente controlados por el atacante. (Dado que el control del usuario sobre este cálculo se limita a un valor de 32 bits sin signo, los sistemas de 64 bits no se ven afectados).

   - El servidor más vulnerable es el KDC, ya que analizará una PAC controlada por el atacante en el controlador S4U2Proxy. El riesgo secundario es para las instalaciones de servidor de archivos habilitadas para Kerberos en un dominio que no es de AD. Un KDC de Heimdal que no sea AD que controle dicho reino puede pasar un PAC controlado por el atacante dentro del ticket de servicio.

3. **Productos afectados:**

   - Versiones de Samba 4.15.x anteriores a la 4.15.12;
   - Versiones de Samba 4.16.x anteriores a 4.16.7;
   - Versiones de Samba 4.17.x anteriores a 4.17.3.

4. Solución:

- El equipo de Samba recomienda actualizar los productos afectados con las últimas versiones de software disponible.
- No hay solución alternativa en sistemas de 32 bits como un controlador de dominio de AD. Los servidores de archivos solo se ven afectados si se encuentran en un dominio que no es de AD. Los sistemas de 64 bits no son explotables.

Fuentes de información	▪ hxxps://www.samba.org/samba/security/CVE-2022-42898.html

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 312	Fecha: 17-11-2022
		Página 10 de 12

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Nueva campaña de phishing que suplanta la identidad de la red social LinkedIn.		
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 campañas maliciosas de envío masivo de correos electrónicos fraudulentos, provenientes de la red social LinkedIn, en el texto del mensaje se advierte una actividad inusual en la cuenta, por lo que será cancelada a menos verifique en el enlace adjunto**,** supuestamente para actualizar los datos personales, con el objetivo robar credenciales de acceso de usuario de LinkedIn.

2. Proceso del ataque phishing:

Imagen 1: Solicitud, para ingresar credenciales de acceso (correo electrónico y contraseña).

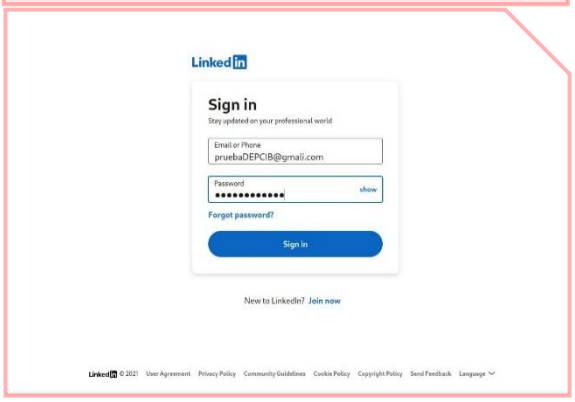
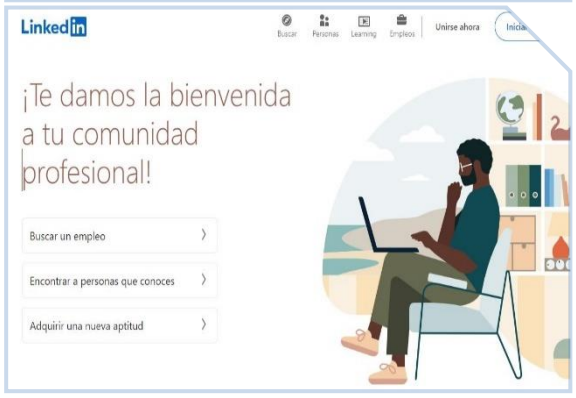
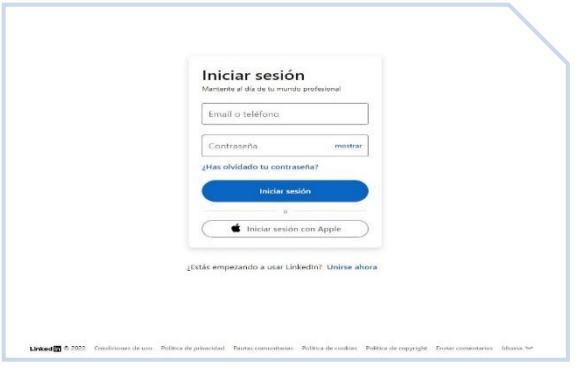


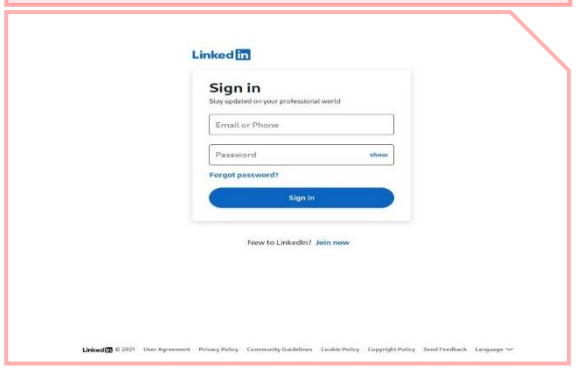
Imagen 2: Una vez ingresado las credenciales de acceso, es redirigido al sitio oficial LinkedIn, aludiendo un aparente error; sin embargo, los datos fueron capturados.



SITIO OFICIAL
URL: https://www.linkedin.com/



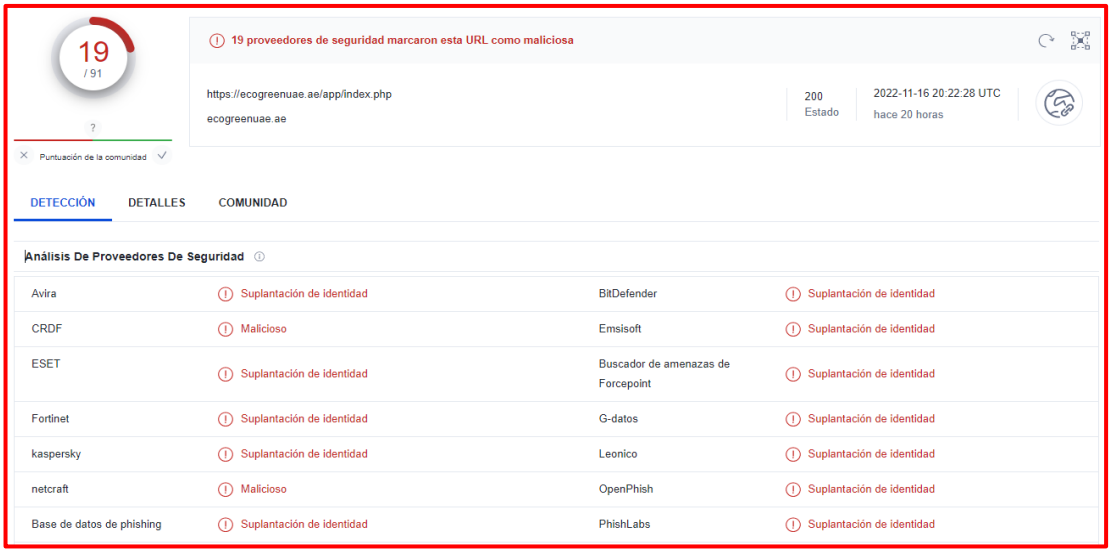
SITIO FRAUDULENTO
URL: hXXps[:]//ecogreenuae[.]ae/app/index[.]php



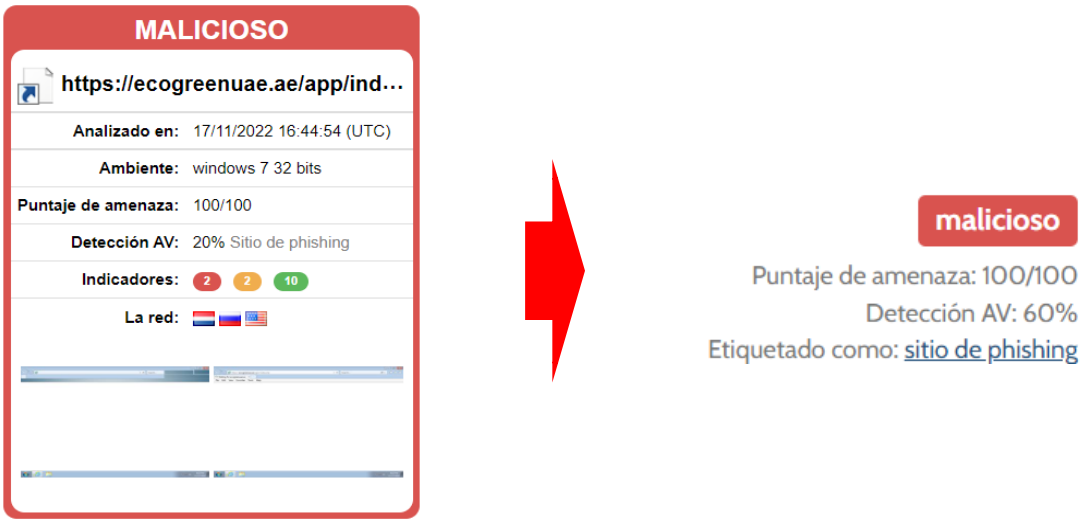
- Existe similitud en imagen de fondo, color y escritura.
- Tiene certificado de seguridad de protocolo HTTPS.
- El dominio se hace pasar por el sitio oficial, pero no coincide.

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

- Indicadores de compromisos:
  - **URL:** hXXps[:]//ecogreenuae[.]ae/app/index[.]php
  - **Dominio:** ecogreenuae[.]ae
  - **Dirección IP:** 184[.]168[.]112[.]132
  - **Código:** 200
  - **Longitud:** 42.23 KB
  - **SHA-256**: 1d9658bec6477d0d77fc85f6557e67652fa161204c476bb864594286a9adbb65



- Otras detecciones del analisis:



4. Recomendaciones:

- Acceder al sitio web a través de fuentes oficiales.
- Evitar responder a mensajes enviados (correo electrónico, Whatsapp, SMS y otros), que contengan enlaces de dudosa procedencia.
- Verificar detenidamente la redacción y ortografía de la dirección URL, que coincidan con el sitio web oficial.
- No compartir la información con terceras personas, amigos o familiares.
- Utilizar un antivirus actualizado ya que es la primera barrera ante un ataque cibernético.

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

Índice alfabético