Instituto de Desarrollo Asegurador

www.evopoliza.com

- Análisis de Vulnerabilidades -

Identificador: 10659
Fecha de Realización: 2020-06-01 14:53:05

Lazarus Technology, S.L.
Calle Teide, 5, 3ª Planta
28703, San Sebastián de los Reyes
Madrid - España
email: info@lazarus.es
tel: +34 91 658 64 16

ISO 9001 2015 CERTIFIED
calidad

Visión General: www.evopoliza.com

0

Vulnerabilidades Graves

Vulnerabilidad de muy fácil explotación que puede poner en riesgo el sistema y los datos que contiene

0

Vulnerabilidades Altas

Vulnerabilidad de fácil explotación que puede poner en riesgo el sistema y los datos que contiene

3

Vulnerabilidades Medias

Vulnerabilidad de compleja explotación, que puede permitir el bloqueo del sistema y robo de información

0

Vulnerabilidades Bajas

Vulnerabilidad de difícil explotación, y que no supone riesgo en si misma pero que combinada con otras puede suponerlo

84

Vulnerabilidades Informativas

Información disponible del sistema, que sin ser un riesgo, permite detectar vulnerabilidades explotables

Lazarus Technology, S.L.
Calle Teide, 5, 3ª Planta
28703, San Sebastián de los Reyes
Madrid - España
email: info@lazarus.es
tel: +34 91 658 64 16

Vulnerabilidades detectadas

Port scanners
Nessus SYN scanner

DESCRIPCIÓN: Este complemento es un escáner de puertos SYN 'medio abierto'. Será razonablemente rápido incluso contra un objetivo con cortafuegos. Tenga en cuenta que los escaneos SYN son menos intrusivos que los escaneos TCP (conexión completa) contra servicios rotos, pero pueden causar problemas para firewalls menos robustos y también dejar conexiones no cerradas en el destino remoto, si la red está cargada.

SOLUCIÓN: Proteja su objetivo con un filtro IP.

Web Servers
Web Application Cookies Not Marked HttpOnly

DESCRIPCIÓN: La aplicación web remota establece varias cookies en la sesión no autenticada y autenticada de un usuario. Sin embargo, una o más de esas cookies no están marcadas como 'HttpOnly', lo que significa que un script malicioso del lado del cliente, como JavaScript, podría leerlas. El indicador HttpOnly es un mecanismo de seguridad para proteger contra ataques de secuencias de comandos entre sitios, que fue propuesto por Microsoft e implementado inicialmente en Internet Explorer. Todos los navegadores modernos ahora lo admiten. Tenga en cuenta que este complemento detecta todas las cookies generales que faltan el indicador de cookies HttpOnly, mientras que el complemento 48432 (Cookies de sesión de aplicación web no marcadas HttpOnly) solo detectará las cookies de sesión de una sesión autenticada que no tenga el indicador de cookies HttpOnly.

SOLUCIÓN: Cada cookie debe revisarse cuidadosamente para determinar si contiene datos confidenciales o si se utiliza para una decisión de seguridad. Si es posible, agregue el atributo 'HttpOnly' a todas las cookies de sesión y a todas las cookies que contengan datos confidenciales.

Web Servers
Web Application Cookies Not Marked Secure

DESCRIPCIÓN: La aplicación web remota establece varias cookies en la sesión no autenticada y autenticada de un usuario. Sin embargo, hay casos en los que la aplicación se ejecuta sobre HTTP sin cifrar o las cookies no están marcadas como "seguras", lo que significa que el navegador podría enviarlas de regreso a través de un enlace no cifrado en ciertas circunstancias. Como resultado, puede ser posible que un atacante remoto intercepte estas cookies. Tenga en cuenta que este complemento detecta todas las cookies generales que faltan el indicador de cookie 'seguro', mientras que el complemento 49218 (Cookies de sesión de aplicación web no marcadas como seguras) solo detectará cookies de sesión de una sesión autenticada que no tenga el indicador de cookie seguro.

SOLUCIÓN: Cada cookie debe revisarse cuidadosamente para determinar si contiene datos confidenciales o si se utiliza para una decisión de seguridad. Si es posible, asegúrese de que todas las comunicaciones se realicen a través de un canal cifrado y agregue el atributo 'seguro' a todas las cookies de sesión o cualquier cookie que contenga datos confidenciales.

Web Servers

DESCRIPCIÓN:

SOLUCIÓN: Consulte con nuestro Servicio Técnico.

Web Servers

Web Server No 404 Error Code Check

DESCRIPCIÓN: El servidor web remoto está configurado de tal manera que no devuelve códigos de error '404 No encontrado' cuando se solicita un archivo inexistente, quizás devolviendo en su lugar un mapa del sitio, una página de búsqueda o una página de autenticación. Lazarus ha habilitado algunas contramedidas para esto. Sin embargo, pueden ser insuficientes. Si se produce una gran cantidad de agujeros de seguridad para este puerto, es posible que no todos sean precisos.

SOLUCIÓN: Consulte con nuestro Servicio Técnico.

Web Servers

External URLs

DESCRIPCIÓN: Lazarus reunió enlaces HREF a sitios externos rastreando el servidor web remoto.

SOLUCIÓN: Consulte con nuestro Servicio Técnico.

CGI abuses

Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header

DESCRIPCIÓN: El servidor web remoto en algunas respuestas establece un encabezado de respuesta antecesores de marco de Política de seguridad de contenido (CSP) permisivo o no establece ninguno en absoluto. El encabezado CSP frame-ancestors ha sido propuesto por el Grupo de trabajo de seguridad de aplicaciones web del W3C como una forma de mitigar los scripts entre sitios y los ataques de clickjacking.

SOLUCIÓN: Establezca un encabezado de antecesores de marco de Política de seguridad de contenido no permisivo para todos los recursos solicitados.

CGI abuses

Missing or Permissive X-Frame-Options HTTP Response Header

DESCRIPCIÓN: El servidor web remoto en algunas respuestas establece un encabezado de respuesta permisivo de X-Frame-Options o no establece ninguno en absoluto. El encabezado X-Frame-Options ha sido propuesto por Microsoft como una forma de mitigar los ataques de clickjacking y actualmente es compatible con todos los principales proveedores de navegadores

SOLUCIÓN: Establezca un encabezado X-Frame-Options configurado correctamente para todos los recursos solicitados.

Web Servers

Web Application Sitemap

DESCRIPCIÓN: El servidor web remoto contiene contenido enlazable que se puede utilizar para recopilar información sobre un objetivo.

SOLUCIÓN: Consulte con nuestro Servicio Técnico.

Web Servers

Web Server Directory Enumeration

DESCRIPCIÓN: Este complemento intenta determinar la presencia de varios directorios comunes en el servidor web remoto. Al enviar una solicitud de un directorio, el código de respuesta del servidor web indica si es un directorio válido o no.

SOLUCIÓN: Consulte con nuestro Servicio Técnico.

Web Servers

Web mirroring

DESCRIPCIÓN: Este complemento crea un espejo de los sitios web remotos y extrae la lista de CGI que utiliza el host remoto. Se sugiere que cambie el número de páginas para reflejar en la sección 'Opciones' del cliente.

SOLUCIÓN: Consulte con nuestro Servicio Técnico.

Web Servers

Web Server Allows Password Auto-Completion

DESCRIPCIÓN: El servidor web remoto contiene al menos un campo de formulario HTML que tiene una entrada de tipo 'contraseña' donde 'autocompletar' no está configurado en 'desactivado'. Si bien esto no representa un riesgo para este servidor web per se, significa que los usuarios que usan los formularios afectados pueden tener sus credenciales guardadas en sus navegadores, lo que a su vez podría conducir a una pérdida de confidencialidad si alguno de ellos usa host o si su máquina se ve comprometida en algún momento.

SOLUCIÓN: Agregue el atributo 'autocomplete = off' a estos campos para evitar que los navegadores almacenen en caché las credenciales.

Web Servers

Web Application Potentially Vulnerable to Clickjacking

DESCRIPCIÓN: El servidor web remoto no establece un encabezado de respuesta X-Frame-Options o un encabezado de respuesta de 'antepasados' de Content-Security-Policy en todas las respuestas de contenido. Esto podría exponer el sitio a un ataque de clickjacking o reparación de la interfaz de usuario, en el que un atacante puede engañar a un usuario para que haga clic en un área de la página vulnerable que es diferente de lo que el usuario percibe que es la página. Esto puede provocar que un usuario realice transacciones fraudulentas o maliciosas. X-Frame-Options ha sido propuesto por Microsoft como una forma de mitigar los ataques de clickjacking y actualmente es compatible con todos los principales proveedores de navegadores. Content-Security-Policy (CSP) ha sido propuesta por el Grupo de trabajo de seguridad de aplicaciones web del W3C, con un apoyo cada vez mayor entre todos los principales proveedores de navegadores, como una forma de mitigar el clickjacking y otros ataques. La directiva de política 'antepasados de marco' restringe qué fuentes pueden incorporar el recurso protegido. Tenga en cuenta que si bien los encabezados de respuesta X-Frame-Options y Content-Security-Policy no son las únicas mitigaciones para el clickjacking, actualmente son los métodos más confiables que se pueden detectar a través de la automatización. Por lo tanto, este complemento puede producir falsos positivos si se implementan otras estrategias de mitigación (por ejemplo, JavaScript que revienta los marcos) o si la página no realiza ninguna transacción sensible a la seguridad.

SOLUCIÓN: Devuelva el encabezado HTTP X-Frame-Options o Content-Security-Policy (con la directiva 'frame-ancestors') con la respuesta de la página. Esto evita que el contenido de la página sea representado por otro sitio cuando se usan las etiquetas HTML de marco o iframe.

Web Servers

HTTP Server Type and Version

DESCRIPCIÓN: Este complemento intenta determinar el tipo y la versión del servidor web remoto.

SOLUCIÓN: Consulte con nuestro Servicio Técnico.

Web Servers

Protected Web Page Detection

DESCRIPCIÓN: El servidor web remoto requiere autenticación HTTP para las siguientes páginas. Hay varios esquemas de autenticación disponibles: - Básico es el más simple, pero las credenciales se envían en texto sin formato. - NTLM proporciona un SSO en un entorno de Microsoft, pero no se puede usar tanto en el proxy como en el servidor web. También es más débil que Digest. - Digest es un esquema criptográficamente fuerte. Las credenciales nunca se envían en texto sin formato, aunque aún pueden ser resquebrajadas por un ataque de diccionario.

SOLUCIÓN: Consulte con nuestro Servicio Técnico.

Web Servers

DESCRIPCIÓN:

SOLUCIÓN: Consulte con nuestro Servicio Técnico.

Settings

Nessus Scan Information

DESCRIPCIÓN: Este complemento muestra, para cada host probado, información sobre el escaneo en sí: - La versión del conjunto de complementos. - El tipo de escáner (Lazarus o Lazarus Home). - La versión del motor Lazarus. - Los escáneres de puerto utilizados. - El rango de puertos escaneado. - Si es posible realizar verificaciones de administración de parches con credenciales o de terceros. - La fecha del escaneo. - La duración del escaneo. - El número de hosts escaneados en paralelo. - El número de comprobaciones realizadas en paralelo.

SOLUCIÓN: Consulte con nuestro Servicio Técnico.

Web Servers

HTTP Methods Allowed (per directory)

DESCRIPCIÓN: Al llamar al método OPTIONS, es posible determinar qué métodos HTTP están permitidos en cada directorio. Los siguientes métodos HTTP se consideran inseguros: PUT, DELETE, CONNECT, TRACE, HEAD Muchos frameworks e idiomas tratan 'HEAD' como una solicitud 'GET', aunque sin un cuerpo en la respuesta. Si se estableció una restricción de seguridad en las solicitudes 'GET' de modo que solo 'Usuarios autenticados' pudieran acceder a las solicitudes GET para un servlet o recurso en particular, se omitiría para la versión 'HEAD'. Esto permitió el envío ciego no autorizado de cualquier solicitud GET privilegiada. Como esta lista puede estar incompleta, el complemento también prueba: si las 'Pruebas exhaustivas' están habilitadas o 'Habilitar pruebas de aplicaciones web' está configurado como 'sí' en la política de escaneo, varios métodos HTTP conocidos en cada directorio y los considera no compatibles si recibe un código de respuesta de 400, 403, 405 o 501. Tenga en cuenta que la salida del complemento es solo informativa y no indica necesariamente la presencia de vulnerabilidades de seguridad.

SOLUCIÓN: Consulte con nuestro Servicio Técnico.

Instituto de Desarrollo Asegurador

178.60.62.166

- Análisis de Vulnerabilidades -

Identificador: 10658
Fecha de Realización: 2020-06-01 14:50:33

Lazarus Technology, S.L.
Calle Teide, 5, 3ª Planta
28703, San Sebastián de los Reyes
Madrid - España
email: info@lazarus.es
tel: +34 91 658 64 16

Visión General: 178.60.62.166

0

Vulnerabilidades Graves

Vulnerabilidad de muy fácil explotación que puede poner en riesgo el sistema y los datos que contiene

0

Vulnerabilidades Altas

Vulnerabilidad de fácil explotación que puede poner en riesgo el sistema y los datos que contiene

1

Vulnerabilidades Medias

Vulnerabilidad de compleja explotación, que puede permitir el bloqueo del sistema y robo de información

0

Vulnerabilidades Bajas

Vulnerabilidad de difícil explotación, y que no supone riesgo en si misma pero que combinada con otras puede suponerlo

12

Vulnerabilidades Informativas

Información disponible del sistema, que sin ser un riesgo, permite detectar vulnerabilidades explotables

Lazarus Technology, S.L.
Calle Teide, 5, 3ª Planta
28703, San Sebastián de los Reyes
Madrid - España
email: info@lazarus.es
tel: +34 91 658 64 16

Vulnerabilidades detectadas

Port scanners
Nessus SYN scanner

DESCRIPCIÓN: Este complemento es un escáner de puertos SYN 'medio abierto'. Será razonablemente rápido incluso contra un objetivo con cortafuegos. Tenga en cuenta que los escaneos SYN son menos intrusivos que los escaneos TCP (conexión completa) contra servicios rotos, pero pueden causar problemas para firewalls menos robustos y también dejar conexiones no cerradas en el destino remoto, si la red está cargada.

SOLUCIÓN: Proteja su objetivo con un filtro IP.

General
Traceroute Information

DESCRIPCIÓN: Hace un trazado de ruta al host remoto.

SOLUCIÓN: Consulte con nuestro Servicio Técnico.

Service detection

DESCRIPCIÓN:

SOLUCIÓN: Consulte con nuestro Servicio Técnico.

Windows

DESCRIPCIÓN:

SOLUCIÓN: Consulte con nuestro Servicio Técnico.

General
OS Identification

DESCRIPCIÓN: Usando una combinación de sondas remotas (por ejemplo, TCP / IP, SMB, HTTP, NTP, SNMP, etc.), es posible adivinar el nombre del sistema operativo remoto en uso. A veces también es posible adivinar la versión del sistema operativo.

SOLUCIÓN: Consulte con nuestro Servicio Técnico.

General
Host Fully Qualified Domain Name (FQDN) Resolution

DESCRIPCIÓN: Lazarus pudo resolver el nombre de dominio completo (FQDN) del host remoto.

SOLUCIÓN: Consulte con nuestro Servicio Técnico.

Settings

Nessus Scan Information

DESCRIPCIÓN: Este complemento muestra, para cada host probado, información sobre el escaneo en sí: - La versión del conjunto de complementos. - El tipo de escáner (Lazarus o Lazarus Home). - La versión del motor Lazarus. - Los escáneres de puerto utilizados. - El rango de puertos escaneado. - Si es posible realizar verificaciones de administración de parches con credenciales o de terceros. - La fecha del escaneo. - La duración del escaneo. - El número de hosts escaneados en paralelo. - El número de comprobaciones realizadas en paralelo.

SOLUCIÓN: Consulte con nuestro Servicio Técnico.

General

TCP/IP Timestamps Supported

DESCRIPCIÓN: El host remoto implementa las marcas de tiempo TCP, según lo definido por RFC1323. Un efecto secundario de esta función es que a veces se puede calcular el tiempo de actividad del host remoto.

SOLUCIÓN: Consulte con nuestro Servicio Técnico.

Firewalls

DESCRIPCIÓN:

SOLUCIÓN: Consulte con nuestro Servicio Técnico.

General

Common Platform Enumeration (CPE)

DESCRIPCIÓN: Al utilizar la información obtenida de un escaneo de Lazarus, este complemento informa las coincidencias de CPE (Common Platform Enumeration) para varios productos de hardware y software que se encuentran en un host. Tenga en cuenta que si un CPE oficial no está disponible para el producto, este complemento calcula el mejor CPE posible en función de la información disponible del escaneo.

SOLUCIÓN: Consulte con nuestro Servicio Técnico.

General

Device Type

DESCRIPCIÓN: Según el sistema operativo remoto, es posible determinar cuál es el tipo de sistema remoto (por ejemplo, una impresora, enrutador, computadora de uso general, etc.).

SOLUCIÓN: Consulte con nuestro Servicio Técnico.

Misc.

DESCRIPCIÓN:

SOLUCIÓN: Consulte con nuestro Servicio Técnico.