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

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Asociación de Bancos del Perú

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

130-2024-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 Aéreadel 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 lasempresas 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°130	Fecha: 04-06-2024
		Página: 4 de 11

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Estafa de la videollamada por WhatsApp		
Tipo de Ataque	Troyanos	Abreviatura	Troyanos
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C02
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

La popularidad de WhatsApp se ha visto empañada recientemente por una nueva táctica empleada por los ciberdelincuentes para infiltrarse en los dispositivos de los usuarios. La función de compartir pantalla, ahora se ha convertido en una vulnerabilidad explotada por los estafadores.

Estafadores se sirven de las tecnologías para cometer sus delitos. Cada cierto tiempo, surge alguna nueva forma que puede tomarnos desprevenidos si no hemos oído hablar de ella, y estamos estresados o despistados en el momento en que nos ponemos a usar nuestra computadora o teléfono móvil.

2. DETALLES:

Esta nueva estafa que se realiza a través de WhatsApp comienza con una videollamada realizada por un desconocido o incluso alguien que se identifica como una persona que te conoce o que te dice que pertenecen al equipo técnico de WhatsApp. Y es que una vez uno acepta la videollamada, el ciberdelincuente no se muestra en cámara, puesto que dice tener algún problema técnico, como una cámara que no transmite imagen, aunque simplemente está tapando su cámara.

Es entonces cuando te pide que, para solucionarlo, presiones sobre el botón de "Compartir pantalla". De esta manera, convence a la víctima de que esta acción corregirá el fallo técnico. Esta estrategia generalmente se dirige a personas con conocimientos técnicos básicos.

Si el usuario cae en la trampa, el malhechor puede ver todo lo que aparece en el dispositivo de la víctima. Este acceso permite al ciberdelincuente enviar un código de seguridad por SMS al teléfono bajo su control. De este modo, pueden ver el código cuando llegue a la víctima y tomar el control de su cuenta de WhatsApp para transferirla a otro dispositivo sin que la otra persona se dé cuenta.

Para meter presión y confundir al estafado recurren siempre a alguna historia en la que están en apuros, es urgente o resulta primordial que reciban el dinero por alguna razón de imperiosa necesidad. Una fórmula efectiva para comprobar si están intentando estafarte de esta forma es llamar por teléfono a la persona que supuestamente te está escribiendo por WhatsApp y preguntarle directamente si es ella.

Más allá de la estafa de compartir pantalla, el phishing continúa como una de las amenazas más persistentes y efectivas en el ciberespacio. Los ataques consisten en el envío de comunicaciones que parecen proceder de fuentes legítimas, con el objetivo de engañar a las personas para que proporcionen información importante. Esto se realiza a menudo mediante correos electrónicos que imitan a bancos, empresas de servicios o plataformas de redes sociales. Los enlaces dentro de estos correos redirigen a las víctimas a sitios web falsos que recogen los datos ingresados.

3. RECOMENDACIONES:

- Utilizar contraseñas seguras que sean extensas y complejas, que combinen letras, números y símbolos.
- Verificar la autenticidad de los sitios web, antes de proporcionar datos personales o financieros.
- Evitar hacer clic en enlaces o descargar archivos adjuntos de fuentes desconocidas.
- Cambiar las contraseñas periódicamente y habilitar la autenticación de dos factores.
- No devolver llamadas a números desconocidos, especialmente aquellos que suenan brevemente y cuelgan.

- Configurar las opciones en la aplicación de WhatsApp en tu celular, habilitando la función para evitar llamadas y videollamadas de números desconocidos. Ello se encuentra en la opción de Ajustes de la aplicación.

  - Encuentra la sección de Privacidad y luego ve hacia Llamadas. Tras ello, deberás activar la opción de "Silenciar llamadas de números desconocidos".
  - Automáticamente, a partir de ese momento, la app no te mostrará las llamadas y videollamadas de este tipo y solo figurarán como llamadas perdidas.

- Usar aplicaciones de identificación de llamadas como Truecaller puede ser de utilidad, para determinar si provienen de telemarketers, estafadores, fraudes, acosadores, y otros tipos de comunicaciones no deseadas. Incluso, para detectar y bloquear robocalls y cualquier otro tipo de spam conocido de manera eficiente.

Fuente de Información:	• hxxps://blog.segu-info.com.ar/2024/06/estafa-de-la-videollamada-por-whatsapp.html • hxxps://www.americatv.com.pe/noticias/util-e-interesante/como-evitar-llamadas-y-videollamadas-desconocidos-whatsapp-n481443 • hxxps://larepublica.pe/tecnologia/2024/05/06/la-nueva-modalidad-de-estafa-por-whatsapp-que-te-roba-tus-datos-bancarios-por-videollamada-y-con-un-solo-clic-evat-118278 • hxxps://elcomercio.pe/tecnologia/redes-sociales/whatsapp-la-nueva-estafa-a-traves-de-videollamadas-que-te-roba-los-datos-bancarios-noticia/?ref=ecr

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°130	Fecha: 04-06-2024
		Página: 6 de 11

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Zyxel lanzó parches de seguridad para múltiples vulnerabilidades críticas en dispositivos NAS		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Zyxel ha lanzado actualizaciones que corrigen múltiples vulnerabilidades de severidad **CRÍTICA** de tipo inyección de comando del sistema operativo, carga sin restricciones de archivos con tipos peligrosos y gestión inadecuada de privilegios que afecta a varios de sus productos. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante no autenticado la inyección de comandos y ejecución remota de código en varios de sus productos NAS que han alcanzado el fin del soporte de vulnerabilidad.

2. DETALLES:

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-29972 de inyección de comandos en el programa CGI “remote_help-cgi” en los dispositivos Zyxel NAS326 y NAS542, podría permitir que un atacante no autenticado ejecute algunos comandos del sistema operativo (SO) enviando una solicitud HTTP POST diseñada.

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-29973 de inyección de comandos en el parámetro "setCookie" en los dispositivos Zyxel NAS326 y NAS542, podría permitir que un atacante no autenticado ejecute algunos comandos del sistema operativo enviando una solicitud HTTP POST diseñada.

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-29974 de ejecución remota de código en el programa CGI “file_upload-cgi” en los dispositivos Zyxel NAS326 y NAS542, podría permitir que un atacante no autenticado ejecute código arbitrario cargando un archivo de configuración diseñado en un dispositivo vulnerable.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-29975 de gestión de privilegios inadecuada en el binario ejecutable SUID en los dispositivos Zyxel NAS326 y NAS542, podría permitir que un atacante local autenticado con privilegios de administrador ejecute algunos comandos del sistema como usuario "root" en un dispositivo vulnerable.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-29976 de administración de privilegios inadecuada en el comando "show_allsessions" en los dispositivos Zyxel NAS326 y NAS542, podría permitir que un atacante autenticado obtenga información de la sesión de un administrador que haya iniciado sesión y que contenga cookies en un dispositivo afectado.

Zyxel lanzó parches de seguridad para estas vulnerabilidades **críticas**, incluso después del final del período de soporte de vulnerabilidades. Tanto NAS326 como NAS542 alcanzaron el fin del soporte de vulnerabilidad el 31 de diciembre de 2023.

A. Productos afectados:

- NAS326, V5.21(AAZF.16)C0 y anteriores.
- NAS542, V5.21(ABAG.13)C0 y anteriores.

3. RECOMENDACIÓN:

- Actualizar los productos afectados a la última versión de software disponible que aborda estas vulnerabilidades.

Fuente de Información:	• hxxps://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-nas-products-06-04-2024

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°130	Fecha: 04-06-2024 Página: 7 de 11

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Exploit para la omisión de autenticación crítica de Progress Telerik		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

La investigadora de ciberseguridad Sina Kheirkha y Soroush Dalili han desarrollado y publicado un script de explotación de prueba de concepto (PoC) que demuestra una vulnerabilidad de ejecución remota de código (RCE) encadenada en los servidores de informes Progress Telerik. Las vulnerabilidades de severidad **CRÍTICA** son de tipo omisión de autenticación y deserialización de datos no confiables. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto la creación de cuentas de administrador sin controles y la ejecución de código arbitrario en servidores vulnerables.

2. DETALLES:

Telerik Report Server es una solución de gestión de informes cifrados de extremo a extremo basada en API que las organizaciones utilizan para agilizar la creación, el intercambio, el almacenamiento, la distribución y la programación de informes.

La investigadora de ciberseguridad Sina Kheirkha desarrolló el exploit con la ayuda de Soroush Dalili y ahora ha publicado un artículo detallado que describe el complicado proceso de explotar dos fallas, una omisión de autenticación y un problema de deserialización, para ejecutar código en el objetivo.

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-4358 de tipo omisión de autenticación podría permitir a un atacante remoto la creación de cuentas de administrador sin controles. La investigadora indicó que amplió la falla al descubrir que se podía acceder al método 'Register' en 'StartupController' sin autenticación, lo que permitía la creación de una cuenta de administrador incluso después de completar la configuración inicial.

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-1800 de tipo deserialización de datos no confiables que permite a atacantes remotos autenticados ejecutar código arbitrario en servidores vulnerables. Un atacante puede enviar una carga útil XML especialmente diseñada con un elemento 'ResourceDictionary' al deserializador personalizado de Telerik Report Server, que utiliza un mecanismo complejo para resolver elementos XML en tipos .NET. El elemento especial en la carga útil utiliza la clase 'ObjectDataProvider' para ejecutar comandos arbitrarios en el servidor, como iniciar 'cmd.exe'.

A. Productos afectados:

- Telerik Report Server 2024, versiones anteriores a Q2 10.1.24.514.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la última versión de software disponible que aborda estas vulnerabilidades.
- Revisar la lista de usuarios de su servidor de informes en busca de nuevos usuarios locales que no reconozcan, agregados en '{host}/Users. /Index.'

Fuente de Información:	• hxxps://summoning.team/blog/progress-report-server-rce-cve-2024-4358-cve-2024-1800/ • hxxps://docs.telerik.com/report-server/knowledge-base/registration-auth-bypass-cve-2024-4358 • hxxps://docs.telerik.com/report-server/knowledge-base/deserialization-vulnerability-cve-2024-1800

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°130	Fecha: 04-06-2024 Página: 8 de 11

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en el módulo MELSEC iQ-R, Q, L Series y MELIPC Series de Mitsubishi Electric		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Se ha reportado una vulnerabilidad de severidad **ALTA** de tipo bloqueo inadecuado de recursos que afecta al Módulo de CPU MELSEC series iQ-R, Q y L, y CPU MELIPC Serie MI5122-VW de Mitsubishi Electric. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto generar una condición de denegación de servicio (DoS) para la comunicación Ethernet. Sería necesario reiniciar el sistema para restaurar la funcionalidad.

2. DETALLES:

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2022-24946 de tipo bloqueo inadecuado de recursos, se debe a que el producto afectado es vulnerable a un desbordamiento de búfer basado en pila, lo que puede permitir a un atacante ejecutar código arbitrario de forma remota.

A. Productos afectados:

- Firmware de CPU MELSEC iQ-R Serie R12CCPU-V: Versión 16 y anteriores.
- MELSEC Serie Q Q03UDECPU: Versiones con los primeros 5 dígitos del número de serie 24061 y anteriores.
- MELSEC Serie Q Q04UDECPU: Versiones con los primeros 5 dígitos del número de serie 24061 y anteriores.
- MELSEC Serie Q Q06UDECPU: Versiones con los primeros 5 dígitos del número de serie 24061 y anteriores.
- MELSEC Serie Q Q10UDECPU: Versiones con los primeros 5 dígitos del número de serie 24061 y anteriores.
- MELSEC Serie Q Q13UDECPU: Versiones con los primeros 5 dígitos del número de serie 24061 y anteriores.
- MELSEC Serie Q Q20UDECPU: Versiones con los primeros 5 dígitos del número de serie 24061 y anteriores.
- MELSEC Serie Q Q26UDECPU: Versiones con los primeros 5 dígitos del número de serie 24061 y anteriores.
- MELSEC Serie Q Q50UDECPU: Versiones con los primeros 5 dígitos del número de serie 24061 y anteriores.
- MELSEC Serie Q Q100UDECPU: Versiones con los primeros 5 dígitos del número de serie 24061 y anteriores.
- MELSEC Serie Q Q03UDVCPU: Versiones con los primeros 5 dígitos del número de serie 24051 y anteriores.
- MELSEC Serie Q Q04UDVCPU: Versiones con los primeros 5 dígitos del número de serie 24051 y anteriores.
- MELSEC Serie Q Q06UDVCPU: Versiones con los primeros 5 dígitos del número de serie 24051 y anteriores.
- MELSEC Serie Q Q13UDVCPU: Versiones con los primeros 5 dígitos del número de serie 24051 y anteriores.
- MELSEC Serie Q Q26UDVCPU: Versiones con los primeros 5 dígitos del número de serie 24051 y anteriores.
- MELSEC Serie Q Q04UDPVCPU: Versiones con los primeros 5 dígitos del número de serie 24051 y anteriores.
- MELSEC Serie Q Q06UDPVCPU: Versiones con los primeros 5 dígitos del número de serie 24051 y anteriores.

- MELSEC Serie Q Q13UDPVCPU: Versiones con los primeros 5 dígitos del número de serie 24051 y anteriores.
- MELSEC Serie Q Q26UDPVCPU: Versiones con los primeros 5 dígitos del número de serie 24051 y anteriores.
- MELSEC Serie Q Q12DCCPU-V: Versiones con los primeros 5 dígitos del número de serie 25061 y anteriores.
- MELSEC Serie Q Q24DHCCPU-V(G): Versiones con los primeros 5 dígitos del número de serie 25061 y anteriores.
- MELSEC Serie Q Q24DHCCPU-LS: Versiones con los primeros 5 dígitos del número de serie 25061 y anteriores.
- MELSEC Serie Q Q26DHCCPU-LS: Versiones con los primeros 5 dígitos del número de serie 25061 y anteriores.
- MELSEC Serie L L02CPU(-P): Versiones con los primeros 5 dígitos del número de serie 24051 y anteriores.
- MELSEC Serie L L06CPU(-P): Versiones con los primeros 5 dígitos del número de serie 24051 y anteriores.
- MELSEC Serie L L26CPU(-P): Versiones con los primeros 5 dígitos del número de serie 24051 y anteriores.
- MELSEC Serie L L26CPU-(P)BT: Versiones con los primeros 5 dígitos del número de serie 24051 y anteriores.
- Firmware de CPU MELIPC Serie MI5122-VW: Versión 05 y anteriores.

3. RECOMENDACIÓN:

- Actualizar los productos afectados a la última versión de firmware disponible que aborda esta vulnerabilidad.

Fuente de Información:	• https://www.cisa.gov/news-events/ics-advisories/icsa-22-172-01

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°130	Fecha: 04-06-2024 Página: 10 de 11

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de inyección de comandos del sistema operativo Oracle WebLogic Server		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Se ha reportado una vulnerabilidad de severidad **CRÍTICA** de tipo inyección de comandos del sistema operativo en Oracle WebLogic Server. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto ejecutar código arbitrario a través de una solicitud HTTP especialmente diseñada que incluye un documento XML malicioso.

2. DETALLES:

La Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA) ha agregado la vulnerabilidad CVE-2017-3506 a su catálogo de vulnerabilidades explotadas conocidas (KEV), citando evidencia de explotación activa.

La agencia indicó, que hay evidencia clara de que la vulnerabilidad CVE-2017-3506 está siendo explotada activamente en la naturaleza, particularmente por el grupo cibercriminal chino 8220 Gang, para implementar software malicioso de minería de criptomonedas en servidores Oracle WebLogic vulnerables.

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2017-3506 de tipo inyección de comandos del sistema operativo Oracle WebLogic Server, podría permitir a un atacante ejecutar código arbitrario a través de una solicitud HTTP especialmente diseñada que incluye un documento XML malicioso. Un atacante no autenticado con acceso a la red a través de HTTP puede comprometer Oracle WebLogic Server. Los ataques exitosos de esta vulnerabilidad pueden resultar en acceso no autorizado a la creación, eliminación o modificación de datos críticos o a todos los datos accesibles de Oracle WebLogic Server.

A. Productos afectados:

- Las versiones compatibles de Oracle WebLogic Server de Oracle Fusion Middleware (subcomponente: Servicios Web) que se ven afectadas son: 10.3.6.0, 12.1.3.0, 12.2.1.0, 12.2.1.1 y 12.2.1.2.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de firmware disponible que aborda esta vulnerabilidad.

Fuente de Información:	• hxxp://www.oracle.com/technetwork/security-advisory/cpuapr2017-3236618.html

Índice alfabético