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

239-2024-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°239	Fecha: 16-10-2024
		Página: 4 de 12

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Detectan troyano bancario que también roba el PIN y el patrón de desbloqueo del smartphone		
Tipo de Ataque	Malware		Malware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C02
Clasificación temática familia	Código Malicioso		

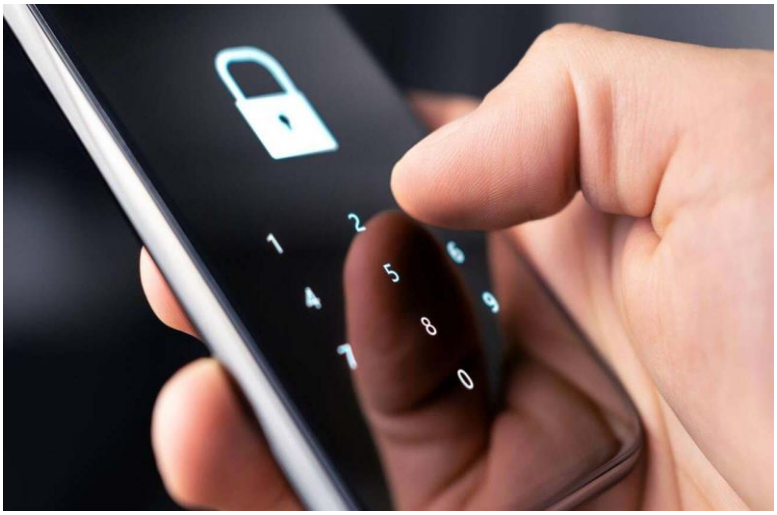
Descripción

1. ANTECEDENTES:

Los ciberdelincuentes cada vez recurren a tácticas cada vez más elaboradas para intentar robar cuentas bancarias, información personal o cualquier cosa que está online.

Desde el quishing, una táctica francamente peligrosa que ha emergido en los últimos meses, o las suplantaciones de identidad, hasta los ya clásicos intentos de phishing que intentan hacerse pasar por páginas que conoces para robarte cualquier cosa.

Un troyano bancario realmente problemático, que ha recibido una actualización que ha hecho saltar todas las alarmas: ahora puede permitir a los ciberdelincuentes robar el PIN o patrón de desbloqueo de un móvil y así controlar un móvil incluso si está bloqueado.



2. DETALLES:

TrickMo es un troyano diseñado para acceder sin autorización a las cuentas bancarias y transacciones financieras de sus víctimas, con el objetivo de robar su dinero. Para ello, es capaz de grabar la pantalla, interceptar los códigos de un solo uso (OTP, por sus siglas en inglés) y conceder permisos de manera automática en las notificaciones emergentes.

El troyano tiene múltiples variantes, como han identificado las firmas de seguridad Cleafy y Zimperium. Esta última, además, ha compartido nuevas capacidades encontradas en las variantes que ha analizado, que apuntan al control del dispositivo móvil incluso cuando está bloqueado.

Algunas muestras tenían la capacidad de robar el PIN o patrón de desbloqueo con una interfaz falsa que simula ser la pantalla de PIN o patrón de desbloqueo del equipo. De esta forma, de manera inadvertida, la víctima introduce su información de desbloqueo de manera natural y sin pensar nada raro, pero el problema es que la información se transmite a los ciberdelincuentes que ya pueden acceder a ese equipo.

TrickMo puede grabar la pantalla del móvil o realizar acciones en remoto para saltarse las solicitudes de los códigos de verificación de dos pasos, de aplicaciones del banco o de compras.

El equipo de ciberseguridad de Zimperium estima que este virus ha afectado al menos a 13.000 dispositivos en todo el mundo.

3. RECOMENDACIONES:

- Evitar abrir o descargar archivos adjuntos o enlaces sospechosos en correos no solicitados o mensajes de redes sociales.
- Controlar tus tarjetas bancarias para hacer seguimiento a las operaciones.
- Cambiar las contraseñas de todas sus cuentas de manera periódica utilizando una contraseña única para cada sitio, y permanecer alerta ante posibles intentos de phishing.
- Utilizar una solución antimalware de confianza en su dispositivo para intervenir si acaba siendo atraído a un sitio web de phishing.
- Aplicar parches y actualizar periódicamente el software y las aplicaciones a su última versión, así como realizar evaluaciones de vulnerabilidad periódicas.
- Capacitar a su equipo en las mejores prácticas de ciberseguridad y manténgalos informados sobre las últimas amenazas.
- Aprender a detectar señales de posibles cambios en el funcionamiento del móvil que pueden alertar la presencia del virus:
  - Si el dispositivo funciona más lento, las aplicaciones tardan en abrirse o la pantalla tarda en responder más de la cuenta, puede estar infectado por un software malicioso.
  - Los cambios en la duración de la batería son otra señal importante. El malware realiza acciones en segundo plano sin que los usuarios lo noten, pero esto agota la batería de forma silenciosa o provoca que se sobrecaliente por el uso.
  - Si descubres que algunas aplicaciones tienen permisos otorgados que no recuerdas haber activado, también debes desconfiar. Los ciberdelincuentes pueden haberlos activado en remoto para acceder a tu información personal y bancaria.
  - Si encuentras una aplicación nueva que no has descargado, podría ser la excusa de los ciberdelincuentes para ejecutar funciones maliciosas en segundo plano desde tu móvil.

Fuente de Información:	• hxxps://www.businessinsider.es/tecnologia/funciona-trickmo-virus-bancario-roba-pin-patron-desbloqueo-movil-1412234 • hxxps://elcomercio.pe/tecnologia/ciberseguridad/ciberseguridad-detectan-troyano-bancario-que-tambien-roba-el-pin-y-el-patron-de-desbloqueo-del-smartphone-trickmo-contrasena-malware-noticia/?ref=ecr • hxxps://computerhoy.20minutos.es/ciberseguridad/trickmo-virus-bancario-te-roba-pin-movil-pantalla-desbloqueo-falsa-puedes-detectarlo-1412320 • hxxps://www.xatakandroid.com/seguridad/detectan-peligroso-malware-bancario-capaz-robarte-pin-movil-mucho-ojo-recibes-sms-mail-asi

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°239	Fecha: 16-10-2024 Página: 6 de 12

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Posible ciberataque al sitio web de la Municipalidad de Miraflores		
Tipo de Ataque	Fuga de Información	Abreviatura	FugaInfo
Medios de propagación	Red, Internet, Redes sociales		
Código de familia	K	Código de Sub familia	K02
Clasificación temática familia	Uso inapropiado de recursos		

Descripción

1. ANTECEDENTES:

El **14 de octubre del 2024**, el equipo de monitoreo de Inteligencia de Ciberamenazas, ha detectado una posible exfiltración de datos que podrían pertenecer a la Municipalidad de Miraflores. El usuario identificado como "akunjwa" registrado en el foro de filtración de datos "LeakBase" desde 07 de mayo del 2024, publicó un anuncio sobre una posible "Fuga de base de datos del Municipio de Miraflores" realizado al sitio web de la institución y tiene a su disposición una base de datos en formato .sql que contiene 82,995 registros de datos personales, y que viene siendo compartido entre los miembros de dicho foro.

2. DETALLES:

El usuario "akunjwa" registrado en el foro de filtración de datos "LeakBase", realizó una publicación donde comparte entre los miembros de dicho foro, un archivo *.sql* con un total de 82,995 registros que posiblemente pertenecen a la Municipalidad de Miraflores.

Publicación de información exfiltrada de la Municipalidad de Miraflores

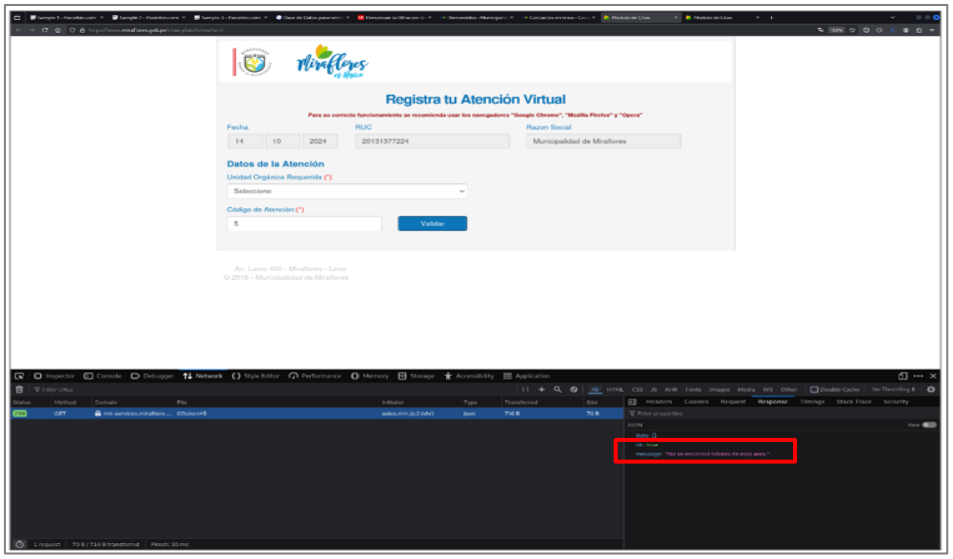
De acuerdo con el análisis realizado al sitio web de la entidad, se detectó que el actor de amenaza podría haber explotado una vulnerabilidad de tipo SQL Injection (SQLi) en el formulario "**Registra tu Atención Virtual**".

Formulario de Atención Virtual

SQL Injection (SQLi) es una técnica de ataque que explota vulnerabilidades en aplicaciones que utilizan bases de datos SQL. A través de la inyección de código SQL malicioso en campos de entrada, un atacante puede manipular consultas a la base de datos para obtener acceso no autorizado a datos sensibles, modificar información o incluso eliminar registros.

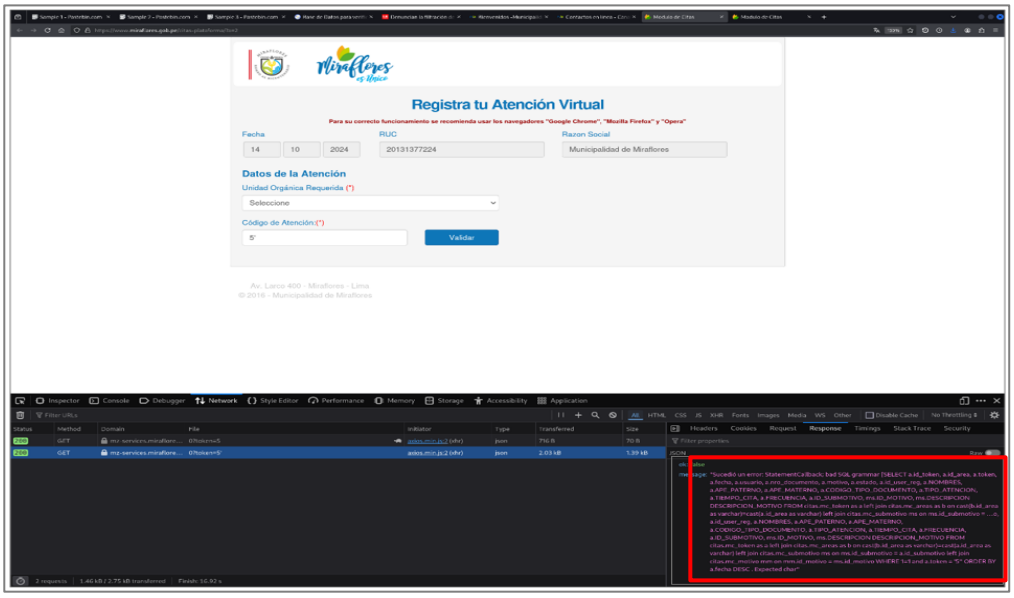
El vector de ataque inicial se da cuando el cibercriminal busca puntos vulnerables en la aplicación donde se aceptan entradas del usuario, como formularios de inicio de sesión o campos de búsqueda. En este caso el formulario vulnerable: "**Registra tu Atención Virtual**".

Luego, se introduce código SQLi en estos campos. En este caso se realizó una prueba de concepto y se realizó una entrada en el campo "Código de Atención", se ingresó el valor "**5**" y nos da como respuesta el siguiente mensaje: "**No se encontró tokens de esta área**".



Formulario de Atención Virtual

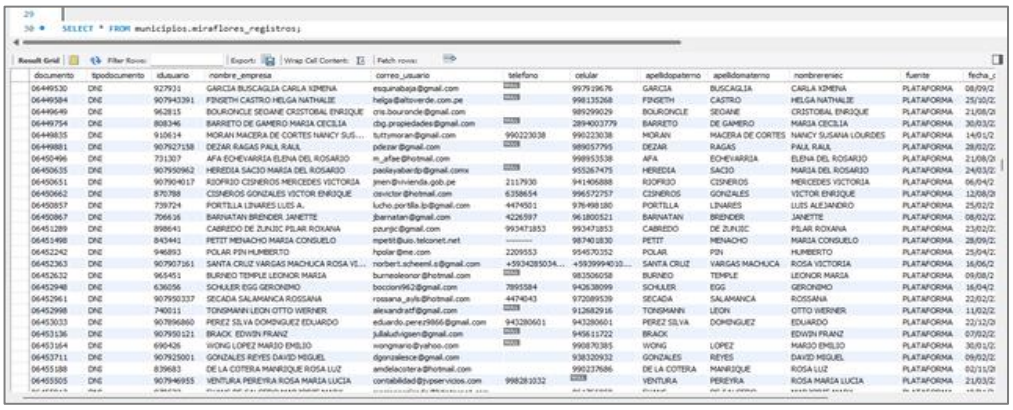
Un atacante remoto puede enviar una solicitud especialmente diseñada a la aplicación afectada y ejecutar comandos SQL arbitrarios dentro de la base de datos de la aplicación. Para este caso, se realizó una entrada con el valor "**5'**", que incluye además el apostrofe, se obtiene como respuesta el mensaje de error que evidenciaría la falla por SQLi. En el cual nos muestra también los campos empleados en la base de datos.



Formulario de Atención Virtual con entrada de código arbitrario

Los campos expuestos por el actor de amenazas en su publicación son:

COLUMNAS: documento, tipodocumento, idusuario, nombre_empresa, correo_usuario, teléfono, celular, representador, apellidopaterno, apellidomaterno, nombrereniec, fuente, fecha_creacion, fecha_modiciacion, usuario_creacion.



En este ataque se pudo evidenciar una vulnerabilidad de tipo SQL Injection, la entrada "**5'**" sugiere que se está intentando realizar una inyección SQL, donde el apóstrofe (') pudo romper la sintaxis de la consulta SQL. Esto llevo a que el sistema ejecute una consulta mal formada, resultando que en la respuesta muestre los campos de la base de datos.

La inyección SQL es una amenaza significativa para la seguridad de las bases de datos, pero con la implementación adecuada de estrategias, es posible reducir considerablemente el riesgo. La combinación de buenas prácticas en la codificación, controles estrictos sobre las entradas del usuario y una infraestructura segura son clave para protegerse contra estos ataques cibernéticos.

A. PRODUCTOS AFECTADOS:

Dominio URL:

- hxxps://www.miraflores.gob.pe/

3. RECOMENDACIONES:

- Validar Datos: Asegurar que todos los datos ingresados por el usuario sean válidos y cumplan con el formato esperado.
- Saneamiento: Escapa o elimina caracteres especiales que puedan ser utilizados para inyecciones SQL, como comillas simples, comillas dobles y otros caracteres que puedan alterar la sintaxis de la consulta.
- Usar consultas preparadas o parametrizadas en lugar de concatenar cadenas para construir consultas SQL. Esto separa los datos del código SQL y previene inyecciones.
- Mensajes de Error Genéricos: no revelar información sensible sobre la estructura de la base de datos en los mensajes de error. Utilizar mensajes genéricos que no proporcionen detalles sobre las consultas fallidas.
- Registro de Errores: implementar un sistema para registrar errores en un archivo seguro o una base de datos para su análisis posterior, sin exponer esta información al usuario final.
- Utilizar herramientas automatizadas en busca de vulnerabilidades comunes, incluida la inyección SQL.
- Implementar firewalls y sistemas de detección de intrusiones (IDS) para monitorear y proteger contra ataques.
- Llevar a cabo pruebas de penetración regularmente para ayudar a identificar vulnerabilidades en su sistema antes de que sean explotadas por atacantes, y así realizar ajustes proactivos en la seguridad.
- Implementar un proceso continuo para validar y sanear las entradas, asegurando que se mantiene la integridad y seguridad del sistema frente a nuevas amenazas.
- Capacitar al personal técnico en las mejores prácticas de seguridad.

Fuente de Información:	Equipo de Trabajo de Seguridad Digital de la DINI

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°239	Fecha: 16-10-2024 Página: 9 de 12

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

Cisco ha publicado múltiples vulnerabilidades de severidad **ALTA** de tipo ejecución con privilegios innecesarios, almacenamiento de contraseñas en un formato recuperable, omisión de autenticación por debilidad primaria, falsificación de solicitud entre sitios (CSRF), Inyección de comando del SO y neutralización incorrecta de etiquetas HTML relacionadas con scripts en una página web (XSS básico) en el firmware del adaptador telefónico analógico Cisco ATA serie 190, tanto local como multiplataforma. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto no autenticado eliminar o cambiar la configuración, ejecutar comandos como usuario root, realizar un ataque de XSS contra un usuario de la interfaz, ver contraseñas, realizar un ataque de CSRF o reiniciar el dispositivo.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-20458 de tipo ejecución con privilegios innecesarios en la interfaz de administración basada en web del firmware del adaptador de teléfono analógico Cisco ATA serie 190, podría permitir que un atacante remoto no autenticado vea o elimine la configuración o cambie el firmware en un dispositivo afectado. Esta vulnerabilidad se debe a la falta de autenticación en puntos finales HTTP específicos. Un atacante podría aprovechar esta vulnerabilidad navegando a una URL específica. Si lo hiciera, podría ver o eliminar la configuración o cambiar el firmware.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-20421 de tipo falsificación de solicitudes entre sitios en la interfaz de administración basada en web del firmware del adaptador de teléfono analógico Cisco ATA serie 190, podría permitir que un atacante remoto no autenticado realice un ataque de CSRF y realice acciones arbitrarias en un dispositivo afectado. Esta vulnerabilidad se debe a que no hay suficientes protecciones CSRF para la interfaz de administración basada en web de un dispositivo afectado. Un atacante podría aprovechar esta vulnerabilidad persuadiendo a un usuario para que siga un enlace creado. Si lo logra, podría permitirle realizar acciones arbitrarias en el dispositivo afectado con los privilegios del usuario objetivo.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-20459 de tipo inyección de comandos en la interfaz de administración basada en web del firmware del adaptador telefónico analógico Cisco ATA 190 Multiplatform Series, podría permitir que un atacante remoto autenticado con altos privilegios ejecute comandos arbitrarios como usuario root en el sistema operativo subyacente. Esta vulnerabilidad se debe a la falta de limpieza de entradas en la interfaz de administración basada en la web. Un atacante podría aprovechar esta vulnerabilidad enviando una solicitud maliciosa a la interfaz de administración basada en la web. Si la explotara con éxito, el atacante podría ejecutar comandos arbitrarios en el sistema operativo subyacente como usuario root. Las vulnerabilidades no dependen unas de otras. No es necesario explotar una de las vulnerabilidades para explotar otra vulnerabilidad. Además, una versión de firmware afectada por una de las vulnerabilidades puede no verse afectada por las otras vulnerabilidades.

Para las vulnerabilidades de severidad **media** identificadas por MITRE se han asignado los siguientes registros: como CVE-2024-20460, CVE-2024-20461, CVE-2024-20462, CVE-2024-20420 y CVE-2024-20463.

Las vulnerabilidades no dependen unas de otras. No es necesario explotar una de las vulnerabilidades para explotar otra vulnerabilidad. Además, una versión de firmware afectada por una de las vulnerabilidades puede no verse afectada por las otras vulnerabilidades.

A. Productos afectados:

Estas vulnerabilidades afectan a los siguientes productos de Cisco si ejecutan una versión vulnerable del firmware local de Cisco ATA 190 Series o del firmware multiplataforma de Cisco ATA 190 Series:

- ATA 191 (local o multiplataforma), versión 12.0.1 y anteriores.
- ATA 192 (multiplataforma), versión 11.2.4 y anteriores.

3. RECOMENDACIÓN:

- Actualizar los paquetes afectados a la última versión disponible que Cisco ha lanzado para abordar esta vulnerabilidad. No existen soluciones alternativas. Sin embargo, existe una mitigación solo para las siguientes vulnerabilidades: CVE-2024-20458, CVE-2024-20421, CVE-2024-20459, CVE-2024-20460, CVE-2024-20463 y CVE-2024-20420. La interfaz de administración basada en web se puede desactivar en el firmware local de Cisco ATA 191. Está desactivada de manera predeterminada.

Fuente de Información:	• hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multi-RDTEqRsy

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°239	Fecha: 16-10-2024 Página: 11 de 12

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de validación de entrada incorrecta en 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 publicado una vulnerabilidad de severidad **ALTA** de tipo validación de entrada incorrecta en Oracle WebLogic Server. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en el producto afectado.

2. **DETALLES:**

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-21216 de tipo validación de entrada incorrecta en Oracle WebLogic Server, podría permitir que un atacante remoto no autenticado ejecute código arbitrario. La vulnerabilidad existe debido a una validación de entrada incorrecta dentro del componente principal de Oracle WebLogic Server. Un atacante remoto no autenticado puede aprovechar esta vulnerabilidad para ejecutar código arbitrario.

A. **Productos afectados:**

- Oracle WebLogic Server: 12.2.1.4.0 - 14.1.1.0.0.

3. **RECOMENDACIÓN:**

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

Fuente de Información:	• hxxps://www.oracle.com/security-alerts/cpuoct2024.html

Índice alfabético