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

022-2025-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°022	Fecha: 27-01-2025
		Página: 4 de 14

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Una vulnerabilidad en WordPress expone a 32.000 páginas a ciberataques		
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 descubierto una vulnerabilidad en WordPress, de tipo asignación incorrecta de privilegios, la cual expone a 32.000 páginas de bienes raíces a ciberataques, debido al widget que lo acompaña.

RealHomes cuenta con más de 32.000 ventas. Además, su versión de pago RealHome es uno de los temas premium para páginas webs inmobiliarias más populares que se ha creado nunca. A los agentes inmobiliarios les gusta especialmente porque cuenta con funciones avanzadas y capacidad de personalización.

2. DETALLES:

La vulnerabilidad, identificada como CVE-2024-32555, corresponde al widget Easy Real Estate, la cual permite a los atacantes iniciar sesión en cualquier cuenta de usuario aprovechando la verificación de correo electrónico insuficiente durante las solicitudes de inicio.

El atacante únicamente requiere la dirección de email de un administrador para obtener acceso no autorizado.

El impacto es grave en la confidencialidad, la integridad y la disponibilidad, todas calificadas como ALTAS. Los atacantes pueden ver datos confidenciales, modificar configuraciones o datos del sistema e interrumpir sus operaciones.

Este problema afecta a las versiones del software Easy Real Estate desde una versión no especificada hasta la 2.2.6.

No hay evidencia de que exista una prueba de concepto pública. No hay evidencia de que se haya probado su explotación por el momento.

3. RECOMENDACIONES:

- Actualizar Easy Real Estate a la versión posterior a la 2.2.6, cuando esté disponible, o desactivarla temporalmente hasta que llegue la versión oficial.
- Auditar periódicamente los privilegios de los usuarios.
- Mantener su sistema operativo, software antimalware y de seguridad, y todas las aplicaciones actualizadas con los últimos parches y actualizaciones de seguridad.
- Habilitar la protección de firewall para monitorear y controlar el tráfico de red entrante y saliente.
- Segmentar las redes para proteger mejor los sistemas críticos.
- Utilizar la política del mínimo privilegio para limitar el número de personas que tienen acceso a un área determinada.

Fuente de Información:	• hxxps://www.escudodigital.com/ciberseguridad/vulnerabilidad-wordpress-expone-paginas-ciberataques_61997_102.html • hxxps://feedly.com/cve/CVE-2024-32555 • hxxps://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2024-32555

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°022	Fecha: 27-01-2025
		Página: 5 de 14

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Vulnerabilidad crítica en Meta Llama Framework permite a atacantes remotos ejecutar código arbitrario		
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:

El equipo de investigación de Oligo ha revelado una vulnerabilidad crítica en el framework LLaMA Stack, desarrollado por Meta, que podría permitir a los atacantes ejecutar código de forma remota (RCE) en sistemas que utilizan esta tecnología. Este framework, ampliamente adoptado en el desarrollo de aplicaciones de inteligencia artificial, representa un riesgo significativo para organizaciones que dependen de él, ya que la vulnerabilidad podría ser explotada para tomar el control de sistemas afectados.

2. DETALLES:

Esta vulnerabilidad, identificada como CVE-2024-50050, permite a atacantes remotos ejecutar código arbitrario en servidores que ejecutan el marco Llama-stack, a través de la deserialización de datos no confiables.

Meta le ha asignado una puntuación de 6,3 sobre 10 (CVSS v3.1), pero la agencia de seguridad de la cadena de suministro de software Snyk, debido a su impacto potencial, le ha asignado puntuaciones de 9,3 (CVSS v4.0) y 9,8 (CVSS v3.1).

Meta presentó el marco Llama-stack en julio de 2024 como una solución de código abierto para simplificar el desarrollo y la implementación de aplicaciones de IA generativa (GenAI) basadas en su familia Llama de modelos de lenguaje grandes (LLM).

Este marco ofrece a los desarrolladores herramientas y API para entrenar, implementar y operar modelos de IA de manera eficiente, lo que permite una innovación más rápida en aplicaciones impulsadas por IA.

La falla reside en un método Python, recv_pyobj, utilizado en el servidor de inferencia Python predeterminado del marco Llama-stack.

Este método recv_pyobj recibe desde un socket un objeto de Python serializado y lo deserializa automáticamente utilizando el módulo pickle de Python.

El formato pickle puede ejecutar cualquier código durante el proceso de deserialización. Esto lo hace inherentemente inseguro, ya que, si el socket está expuesto en la red, un atacante puede construir objetos con código malicioso y enviarlos a través del socket, logrando la ejecución de código remoto (RCE) en la máquina afectada.

Esto abre la puerta a diversas actividades maliciosas, como el robo de recursos, pérdida de datos sensibles, violaciones de datos, acceso no autorizado a sistemas internos, Interrupción de servicios críticos y la manipulación de los modelos de IA alojados.

La vulnerabilidad se debe al uso de la biblioteca pyzmq, una implementación Python del protocolo de mensajería ZeroMQ.

El mantenedor de pyzmq afirma que este uso del método recv_pyobj es, de hecho, inseguro, y recalca: "no debería usarse excepto para fuentes confiables, al igual que el propio pickle. La elección de ejecutarlo en un socket abierto no es una elección de pyzmq, ¡pero parece que meta-llama hizo una elección insegura".

Los equipos de seguridad de Meta han corregido rápidamente la vulnerabilidad en la versión 0.0.41. Según un aviso emitido por Meta, la corrección ha sido cambiar el formato de serialización usado para la comunicación con el socket a JSON. También se ha remediado en la librería pyzmq, actualizando la documentación y los ejemplos para mostrar el uso correcto de recv_pyobj.

3. RECOMENDACIONES:

- Actualizar el framework. Asegurarse de estar utilizando la última versión disponible 0.0.41,
- Realizar un análisis exhaustivo para detectar posibles actividades sospechosas o intentos de explotación.
- Implementar medidas adicionales como firewalls, sistemas de detección de intrusiones (IDS) y monitoreo continuo.
- Seguir las actualizaciones oficiales de Meta y la comunidad de seguridad para estar al tanto de nuevas recomendaciones.

Fuente de Información:	• hxxps://gbhackers.com/critical-vulnerability-in-meta-llama-framework/ • hxxps://unaaldia.hispasec.com/2025/01/fallo-en-el-framework-llama-stack-de-meta-expone-sistemas-de-ia-a-riesgos-de-ejecucion-remota-de-codigo.html • hxxps://thehackernews.com/2025/01/metas-llama-framework-flaw-exposes-ai.html • hxxps://www.infordisa.com/soc/fallo-critico-framework-llama-stack-de-meta/https://www.infordisa.com/soc/fallo-critico-framework-llama-stack-de-meta/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°022	Fecha: 27-01-2025 Página: 7 de 14

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en Microsoft Edge		
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:

Microsoft Corporation ha publicado una vulnerabilidad de severidad **ALTA** de tipo representación errónea de información crítica en la interfaz de usuario (UI) que afecta a Microsoft Edge, específicamente a la versión basada en Chromium. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado explotar el sistema mediante el envío de una entrada manipulada que puede conducir a un acceso no autorizado o a la ejecución de código arbitrario. Esta vulnerabilidad está categorizada como una vulnerabilidad de suplantación de identidad.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-21262 de tipo representación errónea de información crítica en la interfaz de usuario (UI) que afecta a Microsoft Edge, en particular en lo que respecta al manejo inadecuado de la entrada del usuario, podría permitir a un atacante remoto realizar ataques de suplantación de identidad.

Los atacantes pueden manipular la interfaz del navegador, haciendo que parezca que los usuarios están en sitios confiables, como servicios bancarios o de correo electrónico, mientras que en realidad están en dominios maliciosos diseñados para recopilar datos personales, como credenciales de inicio de sesión y detalles financieros.

Esta vulnerabilidad puede aprovecharse junto con esquemas de phishing, en los que se dirige a los usuarios a sitios web falsos que parecen auténticos. Estas tácticas pueden provocar violaciones generalizadas de datos y robo de identidad.

A. Productos afectados:

- Versiones de Microsoft Edge anteriores a 132.0.2957.127.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad.
- Activar las funciones de seguridad integradas, como el filtro SmartScreen y el modo solo HTTPS, que ayudan a identificar y bloquear sitios maliciosos.
- Verificar las URL de los sitios web antes de ingresar información confidencial. Escribir las direcciones manualmente en lugar de hacer clic en los enlaces puede ayudar a evitar intentos de phishing.
- Utilizar contraseñas complejas y considere la posibilidad de utilizar un administrador de contraseñas para generarlas y almacenarlas de forma segura. Esto reduce el riesgo de robo de credenciales.
- Utilizar extensiones de seguridad adicionales como uBlock Origin o HTTPS Everywhere para una mayor protección contra ataques de suplantación de identidad y phishing.

Fuente de Información:	• hxxps://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21262

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°022	Fecha: 27-01-2025
		Página: 8 de 14

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en IBM Storage Copy Data Management para OrientDB		
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:

OrientDB ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo inyección de comando del SO que afecta a IBM Storage Copy Data Management para OrientDB. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado aumentar los privilegios y ejecutar comandos arbitrarios del sistema operativo en el sistema.

2. DETALLES:

OrientDB es un sistema de gestión de bases de datos NoSQL de código abierto escrito en Java, diseñado para admitir múltiples modelos de datos, incluidos los modelos de gráficos, documentos, objetos y clave-valor.

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2017-11467 de tipo inyección de comando del SO que afecta a IBM Storage Copy Data Management para OrientDB. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado aumentar los privilegios y ejecutar comandos arbitrarios del sistema operativo mediante una solicitud especialmente diseñada.

La vulnerabilidad existe debido a que OrientDB no aplica los requisitos de privilegios durante el uso de "where", "fetchplan" u "order by". Un atacante remoto puede ejecutar comandos arbitrarios del sistema operativo mediante una solicitud diseñada.

IBM indicó que hay disponible un exploit público que se puede utilizar para aprovechar esta vulnerabilidad, lo que permite a los atacantes ejecutar comandos arbitrarios en los sistemas afectados sin autenticación. Asimismo, existe un módulo Metasploit para esta vulnerabilidad, diseñado específicamente para explotar la falla de escalada de privilegios en OrientDB. Este módulo puede ejecutar comandos del sistema operativo no protegidos en instalaciones vulnerables.

El código de explotación generalmente implica el envío de solicitudes diseñadas que evitan las verificaciones de privilegios, lo que permite a los atacantes realizar acciones no autorizadas dentro del entorno de la base de datos.

A. Productos afectados:

- IBM Storage Copy Data Management: versiones anteriores a 2.2.25.0.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad.
- Implementar controles de acceso estrictos y supervise de cerca los permisos de los usuarios.
- Auditar periódicamente sus sistemas para verificar el cumplimiento de las mejores prácticas de seguridad.

Fuente de Información:	• hxxps://www.ibm.com/support/pages/node/7177314

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°022	Fecha: 27-01-2025 Página: 9 de 14

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

Cacti Group, Inc. ha publicado múltiples vulnerabilidades de severidad **ALTA** de tipo inyección SQL, error de validación de entrada, exposición a la información e inyección de comandos del sistema operativo. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto no autenticado ejecutar consultas SQL arbitrarias en la base de datos, ejecutar código arbitrario en el sistema, leer, eliminar, modificar datos en la base de datos y obtener control completo sobre la aplicación afectada, obtener acceso a información confidencial y ejecutar comandos de shell arbitrarios en el sistema de destino.

2. DETALLES:

Cacti es una herramienta de monitoreo y gráficos de redes basada en la web y de código abierto, diseñada como una aplicación de interfaz para la herramienta de registro de datos denominada (RRDTool).

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-54146 de tipo inyección SQL, podría permitir a un atacante remoto ejecutar consultas SQL arbitrarias en la base de datos, existe debido a una desinfección insuficiente de los datos proporcionados por el usuario en la función de plantilla del parámetro host_templates.php, Un usuario 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.

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2024-45598 de tipo exposición a la información, podría permitir a un usuario remoto obtener acceso a información potencialmente confidencial, problema de inclusión de archivos locales dentro del parámetro "Poller Standard Error Log Path". Un administrador remoto puede obtener acceso no autorizado a información confidencial en el sistema.

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2024-54145 de tipo inyección SQL, podría permitir a un atacante remoto ejecutar consultas SQL arbitrarias en la base de datos. La vulnerabilidad existe debido a una desinfección insuficiente de los datos proporcionados por el usuario en get_discovery_results función de automation_devices.php. paramter. Un usuario 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.

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-22604 de tipo inyección de comandos del sistema operativo, podría permitir a un usuario remoto ejecutar comandos de shell arbitrarios en el sistema de destino. La vulnerabilidad existe debido a una validación de entrada incorrecta dentro de las respuestas SNMP de varias líneas. Un administrador remoto puede pasar datos especialmente diseñados a la aplicación y ejecutar comandos arbitrarios del sistema operativo en el sistema de destino.

A. Productos afectados:

- Cacti: 1.2.27 / 1.2.28.
- Cacti: 1.2.0 beta1 - 1.2.28; Cacti: 1.2.0 beta1 - 1.2.26.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps://github.com/Cacti/cacti/security/advisories/GHSA-vj9g-p7f2-4wqj • hxxps://github.com/Cacti/cacti/commit/c7e4ee798d263a3209ae6e7ba182c7b65284d8f0 • hxxps://github.com/Cacti/cacti/security/advisories/GHSA-pv2c-97pp-vxwg • hxxps://github.com/Cacti/cacti/commit/eca52c6bb3e76c55d66b1040baa6dbf37471a0ae • hxxps://github.com/Cacti/cacti/security/advisories/GHSA-fh3x-69rr-qqpp • hxxps://github.com/Cacti/cacti/security/advisories/GHSA-c5j8-jxj3-hh36

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°022	Fecha: 27-01-2025 Página: 10 de 14

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidades en SUSE para el kernel de Linux		
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:

SUSE Linux ha publicado dos vulnerabilidades de severidad **ALTA** de tipo uso después de la liberación que afectan a múltiples paquetes de SUSE para el kernel de Linux. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto ejecutar código arbitrario en el sistema. Igualmente, un usuario local podría aumentar privilegios en el sistema de destino.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-36971 de tipo uso después de la liberación que afectan a varios paquetes de SUSE para el kernel de Linux, podría permitir a un atacante remoto ejecutar código arbitrario en el sistema. La vulnerabilidad existe debido a un error de uso después de la liberación dentro de la función xfrm_link_failure() en net/xfrm/xfrm_policy.c, dentro de las funciones dst_entry ip6_dst_check() e ip6_dst_check() en net/ipv6/route.c, dentro de las funciones dst_entry ipv4_dst_check() e ip_do_redirect() en net/ipv4/route.c. Un atacante remoto puede enviar paquetes especialmente diseñados al sistema y ejecutar código arbitrario.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-41057 de tipo uso después de la liberación que afectan a varios paquetes de SUSE para el kernel de Linux, podría permitir a un usuario local aumentar privilegios en el sistema. La vulnerabilidad existe debido a un error de uso posterior a la liberación dentro de la función cachefiles_free_volume() en fs/cachefiles/volume.c, dentro de las funciones cachefiles_withdraw_objects() y cachefiles_withdraw_cache() en fs/cachefiles/cache.c.

Estas vulnerabilidades pueden explotarse localmente y están siendo explotadas activamente en la naturaleza. El atacante debe tener credenciales de autenticación y autenticarse correctamente en el sistema.

A. Productos afectados:

- SUSE Linux Enterprise Server para SAP Applications 15: SP3 / SP5.
- SUSE Linux Enterprise Server 15: SP3 / SP5.
- SUSE Linux Enterprise High Performance Computing 15: SP3 / SP5.
- SUSE Linux Enterprise Micro: 5.1 - 5.2 / SUSE Linux Enterprise Micro: 5.5.
- SUSE Linux Enterprise Live Patching: 15-SP5.
- SUSE Linux Enterprise Real Time 15: SP5.
- OpenSuse Leap: 15.3 / openSUSE Leap: 15.5.
- kernel-livepatch-5_3_18-150300_59_150-preempt-debuginfo: anterior a 15-150300.2.1.
- kernel-livepatch-5_3_18-150300_59_150-preempt: anterior a 15-150300.2.1.
- kernel-livepatch-SLE15-SP3_Update_41-debugsource: anterior a 15-150300.2.1.
- kernel-livepatch-5_3_18-150300_59_150-default: anterior a 15-150300.2.1.
- kernel-livepatch-5_3_18-150300_59_150-default-debuginfo: anterior a 15-150300.2.1.
- kernel-livepatch-5_14_21-150500_55_44-default-debuginfo: anterior a 15-150500.2.1.
- kernel-livepatch-SLE15-SP5_Update_9-debugsource: anterior a 15-150500.2.1.
- kernel-livepatch-5_14_21-150500_55_44-default: anterior a 15-150500.2.1.

3. RECOMENDACIONES:

- Actualizar los paquetes de los productos afectados a la última versión disponible que abordan estas vulnerabilidades.
- Aplicar mitigaciones según las instrucciones del proveedor o suspender el uso del producto.

Fuente de Información:	• hxxp://www.suse.com/support/update/announcement/2025/suse-su-20250241-1/ • hxxp://www.suse.com/support/update/announcement/2025/suse-su-20250242-1/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°022	Fecha: 27-01-2025 Página: 11 de 14

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Apple lanzó actualizaciones de seguridad que corrigen una vulnerabilidad de día cero		
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:

Apple Inc. ha lanzado actualizaciones de seguridad que corrige una vulnerabilidad **CRÍTICA** de día cero de tipo desbordamiento de búfer basada en pila que afecta al componente CoreMedia de Apple, específicamente a iOS, macOS, tvOS y watchOS. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado obtener privilegios elevados, lo que podría permitirle ejecutar código arbitrario con permisos superiores a los previstos.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-24085 de tipo desbordamiento de búfer basada en pila que afecta específicamente a iOS, macOS, tvOS y watchOS, podría permitir a un atacante remoto no autenticado obtener privilegios elevados, lo que podría permitirle ejecutar código arbitrario con permisos superiores a los previstos.

La vulnerabilidad plantea riesgos importantes para los datos de los usuarios debido a la escalada de privilegios dentro del componente CoreMedia de Apple. Un atacante podría obtener acceso no autorizado a datos confidenciales del usuario almacenados en el dispositivo, incluida información personal, archivos y datos de aplicaciones, modificar o eliminar datos del usuario, lo que provocaría la pérdida o corrupción de datos. Asimismo, la vulnerabilidad podría permitir que una aplicación determine la ubicación actual de un usuario sin su consentimiento, lo que podría conducir al seguimiento no autorizado de los usuarios.

Apple tiene conocimiento de un informe que indica que este problema podría haberse explotado activamente en versiones de iOS anteriores a iOS 17.2.

A. Productos afectados:

- iOS, versiones anteriores 18.3.
- iPhone XS y modelos posteriores.
- iPad Pro (13 pulgadas y posteriores).
- iPad Pro (12,9 pulgadas, 3.ª generación y posteriores).
- iPad Pro (11 pulgadas, 1.ª generación y posteriores).
- iPad Air (3.ª generación y posteriores).
- iPad (7.ª generación y posteriores).
- iPad mini (quinta generación y posteriores).
- macOS Sequoia.
- Apple Watch Series 6 y posteriores.
- Apple TV HD y Apple TV 4K (todos los modelos).

3. RECOMENDACIONES:

- Actualizar los dispositivos afectados a la versión de iOS 18.3 que corrige esta vulnerabilidad. La actualización incluye una gestión de memoria mejorada y comprobaciones que ayudan a prevenir la explotación de la vulnerabilidad.
- Utilizar la autenticación multifactor (MFA) para agregar una capa adicional de seguridad, dificultando el acceso de usuarios no autorizados.

Fuente de Información:	• hxxps://developer.apple.com/documentation/coremedia • hxxps://9to5mac.com/2025/01/27/update-your-iphone-ipad-and-mac-now-to-fix-these-security-issues/ • hxxps://support.apple.com/en-us/122066

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°022	Fecha: 27-01-2025 Página: 12 de 14

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Nueva campaña "J-magic" dirigido a enrutadores empresariales Juniper		
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:

Investigadores de Black Lotus Labs de Lumen Technologies han descubierto una nueva campaña maliciosa de malware dirigida a los enrutadores Juniper de nivel empresarial llamada J-magic. La operación, que comenzó a mediados de 2023, explotó vulnerabilidades en JunoOS de Juniper. Un ataque exitoso podría permitir a un atacante obtener el control total sobre el dispositivo comprometido, así como el robo de datos e implementar algún tipo de malware para posteriores ataques.

2. DETALLES:

Black Lotus Labs indico que el ataque utiliza un agente pasivo que monitorea el tráfico TCP en busca de un "Magic Packet" específico enviado por el atacante. Una vez que se detecta este paquete, el agente activa un desafío secundario antes de establecer un shell inverso en el enrutador comprometido, lo que otorga a los atacantes control total sobre el dispositivo vulnerable. Con este acceso, los actores de amenazas pueden robar datos confidenciales o implementar software malicioso.

Los investigadores de Black Lotus Labs dijeron que los enrutadores Juniper que ejecutan JunoOS son sus principales objetivos debido a su ubicación dentro de las redes corporativas. Una vez que un dispositivo se ve comprometido, el atacante obtiene la capacidad de exfiltrar datos, robar credenciales o usar el dispositivo como punto de apoyo para otros sistemas internos.

El malware involucrado en la campaña J-magic parece ser una variante personalizada de cd00r, una puerta trasera de código abierto lanzada originalmente en 2000. Cd00r se ha utilizado en varias campañas debido a su capacidad para explotar vulnerabilidades en sistemas en red. Una vez instalado, el malware escucha un "Magic Packet" y, si se cumplen las condiciones, crea una conexión de shell inversa con la máquina del atacante. Luego, el atacante envía un desafío protegido criptográficamente para autenticarse y obtener más acceso al sistema.

cd00r es un malware de puerta trasera sofisticado que ataca principalmente a los sistemas operativos UNIX. Funciona monitoreando el tráfico de la red en busca de patrones específicos, a los que se refiere como un "golpe secreto", para activar y otorgar acceso remoto a los atacantes. Este método de operación único lo distingue de las puertas traseras tradicionales que generalmente escuchan en un puerto designado.

La telemetría de Black Lotus Labs indica que J-magic ha afectado a una amplia gama de sectores, incluidos la energía, la fabricación de semiconductores y la TI, con un enfoque notable en las empresas de infraestructura crítica. En particular, aproximadamente el 50% de los enrutadores comprometidos estaban configurados como puertas de enlace VPN, lo que permite el acceso remoto a las redes comprometidas.

Uno de los aspectos más notables de la campaña es el enfoque en los enrutadores Juniper. Si bien se ha visto un fuerte ataque a otros equipos de red, esta campaña demuestra que los atacantes pueden tener éxito al expandirse a otros tipos de dispositivos, como los enrutadores de nivel empresarial. El malware "Magic Packet" se esté convirtiendo en una tendencia creciente en el uso contra dispositivos perimetrales, primero con BPFdoor y Symbiote.

La evolución de cd00r en variantes como J-magic ilustra la creciente sofisticación del malware y los desafíos que enfrentan los profesionales de la ciberseguridad para detectar y mitigar dichas amenazas.

A. Productos afectados:

- Routers Juniper, múltiples versiones.

B. Indicadores de compromiso (IoC):

- sha1:7edc911b31b4f5dc401725c9b52e876a9fd00f3e
- sha256:5e3c128749f7ae4616a4620e0b53c0e5381724a790bba8314acb502ce7334df2
- sha256:957c0c135b50d1c209840ec7ead60912a5ccefd2873bf5722cb85354cea4eb37
- sha256:3f26a13f023ad0dcd7f2aa4e7771bba74910ee227b4b36ff72edc5f07336f115
- sha256:C7cf51499973908cbc4c746f689b6ed245b26b1a9eae62fe9329f3a1036e82f4
- IP: 198.46.158[.]172
- Nombres de procesos: [nfsiod 0] / [nfsiod 0].

3. RECOMENDACIONES:

- Utilizar herramientas de monitoreo de red para detectar patrones inusuales en el tráfico que puedan indicar la presencia de un backdoor como cd00r. Un aumento en el tráfico o conexiones inesperadas puede ser una señal de alerta.
- Implementar cortafuegos robustos que puedan rastrear y filtrar el tráfico entrante y saliente. Los sistemas de detección y prevención de intrusiones (IDS/IPS) también son útiles para identificar comportamientos sospechosos en la red y bloquear accesos no autorizados.
- Mantener todos los dispositivos y software actualizados con las últimas correcciones de seguridad. Esto ayuda a cerrar vulnerabilidades que podrían ser explotadas por malware como cd00r.
- Instalar software antivirus y antimalware confiable que ofrezca protección en tiempo real contra amenazas avanzadas. Estas herramientas pueden detectar y bloquear intentos de acceso no autorizados antes de que causen daños.
- Implementar contraseñas fuertes y considera el uso de autenticación de dos factores (2FA) para añadir una capa adicional de seguridad a las cuentas críticas.
- Realizar auditorías periódicas y revisiones de seguridad para identificar posibles brechas en la infraestructura y corregirlas antes de que sean explotadas.
- Dividir la red en subredes más pequeñas para limitar el acceso a datos sensibles y reducir el impacto en caso de una brecha de seguridad.
- Limitar el acceso a información sensible según las necesidades laborales, asegurando que solo personal autorizado tenga acceso a herramientas críticas.
- Aislar todos los dispositivos críticos dentro de la red para limitar el acceso a ellos y reducir el riesgo en caso de un ataque exitoso.
- Realizar análisis regulares en busca de malware en todos los archivos y sistemas. Utiliza múltiples motores antivirus para mejorar la tasa de detección.
- Capacitar a los usuarios sobre los riesgos del malware y las mejores prácticas para evitar caer en trampas como descargas no verificadas o enlaces sospechosos.

Fuente de Información:	• hxxps://blog.lumen.com/the-j-magic-show-magic-packets-and-where-to-find-them/ • hxxps://www.cybersecurity-help.cz/blog/4527.html • hxxps://github.com/blacklotuslabs/IOCs/blob/main/Jmagic_IOCs.txt

Índice alfabético