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

221-2024-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°221	Fecha: 24-09-2024
		Página: 4 de 9

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	El malware para Android 'Necro' infecta 11 millones de dispositivos a través de Google Play		
Tipo de Ataque	Troyanos	Abreviatur	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:

Los dispositivos móviles son un objetivo claro para los piratas informáticos. Si logran colar algún tipo de malware, podrían robar contraseñas, datos personales o controlarlos remotamente.

Justamente han infectado millones de dispositivos Android. Para ello han utilizado Google Play, a través de versiones modificadas de softwares muy utilizados, como es el caso de WhatsApp o Spotify.

También han modificado otras aplicaciones legítimas, así como juegos, para lograr infectar el dispositivo.

Un Troyano es un tipo de malware que se disfraza de software legítimo para engañar a los usuarios y hacer que lo instalen. Su nombre proviene de la historia del caballo de Troya, ya que, al igual que este, el troyano se presenta como algo inofensivo, pero una vez instalado, puede llevar a cabo acciones dañinas, como robar información personal, instalar otros tipos de malware o dar acceso remoto al sistema afectado.

2. DETALLES:

Este malware se denomina Necro. Éste instala varias cargas útiles en los dispositivos infectados y activa varios complementos maliciosos, incluidos:

- Adware que carga anuncios intrusivos a través de ventanas WebView invisibles (complemento Island, Cube SDK).
- Módulos que descargan y ejecutan archivos maliciosos JavaScript y DEX arbitrarios (Happy SDK, Jar SDK).
- Herramientas diseñadas específicamente para facilitar el fraude suscribiendo a los usuarios a servicios de pago sin su conocimiento (complemento web, Happy SDK, complemento Tap).
- Mecanismos que utilizan dispositivos infectados como servidores proxy para enrutar tráfico malicioso (complemento NProxy).

Kaspersky descubrió la presencia de Necro Loader en dos aplicaciones en Google Play, ambas con una base de usuarios sustancial.

La primera es Wuta Camera de Benqu, una herramienta de edición y embellecimiento de fotografías con más de 10.000.000 de descargas en Google Play.

Los analistas de amenazas informan que Necro apareció en la aplicación con el lanzamiento de la versión 6.3.2.148 y permaneció integrado hasta la versión 6.3.6.148, momento en el que Kaspersky notificó a Google.

Si bien el troyano fue eliminado en la versión 6.3.7.138, cualquier carga útil que pudiera haberse instalado a través de versiones anteriores aún podría estar presente en los dispositivos Android.

La segunda aplicación legítima que transportaba Necro es Max Browser de 'WA message recover-wamr', que tenía 1 millón de descargas en Google Play hasta que fue eliminada, tras el informe de Kaspersky.

Kaspersky afirma que la última versión de Max Browser, 1.2.0, todavía incluye Necro, por lo que no hay una versión limpia disponible para actualizar, y se recomienda a los usuarios del navegador web que lo desinstalen inmediatamente y cambien a otro navegador.

Kaspersky dice que las dos aplicaciones fueron infectadas por un SDK publicitario llamado 'Coral SDK', que empleó ofuscación para ocultar sus actividades maliciosas y también esteganografía de imágenes para descargar la carga útil de segunda etapa, shellPlugin, disfrazada de imágenes PNG inofensivas

El troyano Necro se propaga principalmente a través de versiones modificadas de aplicaciones populares (mods) que se distribuyeron a través de sitios web no oficiales.

Entre los ejemplos más destacados que ha descubierto Kaspersky se encuentran los mods de WhatsApp 'GBWhatsApp' y 'FMWhatsApp', que prometen mejores controles de privacidad y límites ampliados para compartir archivos. Otro es el mod de Spotify, 'Spotify Plus', que promete acceso gratuito a servicios premium sin publicidad.

El informe también menciona mods de Minecraft y mods para otros juegos populares como Stumble Guys, Car Parking Multiplayer y Melon Sandbox, que fueron infectados con el cargador Necro.

En todos los casos, el comportamiento malicioso fue el mismo: mostrar anuncios en segundo plano para generar ingresos fraudulentos para los atacantes, instalar aplicaciones y APK sin el consentimiento del usuario y utilizar WebViews invisibles para interactuar con servicios pagos.

3. RECOMENDACIONES:

- Eliminar cualquiera de esas dos aplicaciones, en caso de que las tengas instaladas. A partir de ahí, también debes tener mucho cuidado con instalar modificaciones de WhatsApp o cualquier aplicación.
- Mantener el software actualizado. Actualizar periódicamente los sistemas operativos, las aplicaciones y el software de seguridad para corregir las vulnerabilidades.
- Utilizar un software antimalware confiable en sus dispositivos y mantenerlos actualizados.
- No hacer clic en enlaces sospechosos y sólo descargar aplicaciones únicamente de fuentes oficiales como Google Play Store.
- 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.
- Habilitar la autenticación de dos factores cuando esté disponible.
- Activar Play Protect para realizar un control de seguridad sobre las aplicaciones antes que sean instaladas. Además, Play Protect puede analizar tu dispositivo en busca de aplicaciones maliciosas una vez instaladas y te notifica si detecta que alguna app podría estar accediendo a tu información personal. Para activar realizar los siguientes pasos:
  - Abre Google Play Store.
  - Toca el icono de tu perfil en la esquina superior derecha.
  - Ve a Play Protect y entra a Configuración.
  - Activa la opción "Analizar las apps con Play Protect".
- Capacitar a los usuarios sobre las mejores prácticas de ciberseguridad.

Fuente de Información:	• hxxps://www.bleepingcomputer.com/news/security/android-malware-necro-infects-11-million-devices-via-google-play/ • hxxps://www.redeszone.net/noticias/seguridad/millones-moviles-infectados-evitar/ • hxxps://rpp.pe/tecnologia/apps/ciberseguridad-que-es-necro-y-que-cuidados-tener-ante-amenaza-que-ha-infectado-11-millones-de-usuarios-de-android-noticia-1586747?ref=rpp • hxxps://computerhoy.com/ciberseguridad/11-millones-moviles-android-infectados-malware-infiltrado-play-store-1406570

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°221	Fecha: 24-09-2024 Página: 6 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en el complemento MDTF para WordPress		
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 **CRÍTICA** de tipo inyección SQL que afecta al complemento MDTF (filtro de metadatos y taxonomías) para WordPress. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante autenticado ejecutar comandos SQL arbitrarios, lo que podría comprometer la base de datos y exponer información confidencial.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2024-8624 de tipo inyección SQL en el complemento MDTF para WordPress a través del atributo 'meta_key' del shortcode 'mdf_select_title', podría permitir a un atacante autenticado con acceso de nivel de colaborador y superior agregar consultas SQL adicionales a las consultas existentes. Esto se puede aprovechar para extraer información confidencial de la base de datos. Los atacantes podrían acceder, modificar o eliminar datos confidenciales almacenados en la base de datos de WordPress.

A. Productos afectados:

- Complemento MDTF para WordPress hasta la versión 1.3.3.3.

3. RECOMENDACIONES:

- Actualizar a la última versión el complemento que soluciona esta vulnerabilidad;
- Desactivar temporalmente el complemento MDTF si no es crítico en las operaciones;
- Implementar controles de acceso sólidos para limitar la cantidad de usuarios con acceso de nivel de colaborador o superior;
- Usar reglas de firewall de aplicaciones web (WAF) para detectar y bloquear intentos de inyección SQL;
- Auditar y monitorear regularmente las actividades de la base de datos para detectar consultas sospechosas o intentos de acceso no autorizado;
- Mantener actualizados el núcleo, los temas y otros complementos de WordPress para minimizar la exposición general a vulnerabilidades.

Fuente de Información:	• hxxps://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3153150%40wp-meta-data-filter-and-taxonomy-filter&new=3153150%40wp-meta-data-filter-and-taxonomy-filter • hxxps://www.wordfence.com/threat-intel/vulnerabilities/id/8f50812a-c6a7-4bb3-9833-e10acd0460c0?source=cve

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°221	Fecha: 24-09-2024 Página: 7 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en IBM Tivoli Business Service Manager		
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 neutralización incorrecta de la entrada durante la generación de páginas web (Cross-site Scripting) que afecta a IBM Tivoli Business Service Manager. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado robar información confidencial, cambiar la apariencia de la página web, realizar ataques de phishing y de descarga automática.

2. DETALLES:

IBM Tivoli Business Service Manager (TBSM) es una solución integral de gestión de servicios diseñada para mejorar la visibilidad y el control de los servicios empresariales y su infraestructura de TI subyacente.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2008-7220 de tipo Cross-site scripting, podría permitir a un atacante remoto realizar ataques de secuencias de comandos entre sitios (XSS). La vulnerabilidad existe debido a una limpieza insuficiente de los datos proporcionados por el usuario. Un atacante remoto puede engañar a la víctima para que siga un enlace especialmente diseñado y ejecute código HTML y script arbitrario en el navegador del usuario en el contexto de un sitio web vulnerable.

La explotación exitosa de esta vulnerabilidad puede permitir a un atacante remoto robar información potencialmente confidencial, cambiar la apariencia de la página web, realizar ataques de phishing y de descarga automática.

A. Productos afectados:

- IBM Tivoli Business Service Manager: versiones anteriores a 6.2.0.5.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxp://www.ibm.com/support/pages/node/7168727

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°221	Fecha: 24-09-2024 Página: 8 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades en Red Hat JBoss Core Services Apache HTTP 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:

Red Hat ha publicado múltiples vulnerabilidades de severidad **ALTA** de tipo falsificación de solicitud del lado del servidor (SSRF) y división de la respuesta HTTP que afecta a Red Hat JBoss Core Services Apache HTTP Server. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto no autenticado realizar ataques SSRF y ataques de división de HTTP.

2. DETALLES:

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2024-38472 de tipo SSRF, podría permitir a un atacante remoto realizar ataques SSRF. La vulnerabilidad existe debido a una validación insuficiente de la información proporcionada por el usuario. Un atacante remoto puede enviar una solicitud HTTP especialmente diseñada y engañar al servidor web para que filtre los hashes NTLM. Tenga en cuenta que la vulnerabilidad afecta únicamente a las instalaciones de Windows.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-40898 de tipo SSRF, podría permitir a un atacante remoto realizar ataques SSRF. La vulnerabilidad existe debido a una validación insuficiente de la entrada proporcionada por el usuario en Apache HTTP Server en Windows con mod_rewrite en el contexto de servidor/host virtual. Un atacante remoto puede obligar al servidor web a filtrar hashes NTML a un servidor malicioso a través de SSRF y solicitudes maliciosas.

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2023-38709 de tipo división de la respuesta HTTP, podría permitir a un atacante remoto realizar ataques de división de HTTP. La vulnerabilidad existe debido a que el software no procesa correctamente las secuencias de caracteres CRLF. Un generador de contenido o backend malintencionado o explotable puede enviar una respuesta especialmente diseñada que contenga una secuencia CRLF y hacer que la aplicación envíe una respuesta HTTP dividida. La explotación exitosa de la vulnerabilidad podría permitir a un atacante realizar un ataque de envenenamiento de caché.

A. Productos afectados:

- JBoss Core Services: before 2.4.57 SP6.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible que aborda estas vulnerabilidades.

Fuente de Información:	• hxxp://access.redhat.com/errata/RHSA-2024:6928

Índice alfabético