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

249-2024-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°249	Fecha: 28-10-2024 Página: 4 de 9

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	El peligro del 'smishing': ciberdelincuentes intensifican el uso de mensajes SMS para fraudes en Perú		
Tipo de Ataque	Phishing		Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Sub familia	G01
Clasificación temática familia	Fraude		

Descripción

1. ANTECEDENTES:

Hay una preocupación en ascenso por la proliferación de este delito informático y destacan la necesidad urgente de la implementación de medidas.

El fraude informático, especialmente a través de celulares robados, se ha convertido en uno de los delitos más frecuentes en el Perú. Según datos recientes, el 2023 marcó un récord de denuncias, con 21.842 casos presentados ante las fiscalías provinciales penales y mixtas del país. Esto representa un incremento del 58 % respecto al año anterior, de acuerdo con el diario El Peruano.

2. DETALLES:

Uno de los delitos más comunes es el smishing. Según Erick Iriarte, abogado experto en legislación informática, este fraude "es un ataque de ingeniería social que utiliza mensajes de texto móviles falsos para engañar a las personas para que descarguen un virus, compartan información confidencial o envíen dinero a un delincuente".

Estos mensajes de texto parecen legítimos y provenientes de fuentes confiables como bancos, empresas de servicios o incluso entidades gubernamentales, y suelen alertar al receptor sobre situaciones urgentes que requieren atención inmediata, como problemas con cuentas bancarias o paquetes pendientes de entrega.

A menudo, a través de esta modalidad, se incita al destinatario a hacer clic en un enlace. Sin embargo, el enlace conduce a un sitio web falso diseñado para obtener datos sensibles o incluso instalar software malicioso en el dispositivo del usuario.

Detallando el desarrollo de un Smishing:

- Recepción del mensaje: La víctima recibe un mensaje de texto en su teléfono móvil. El mensaje puede parecer provenir de una fuente confiable, como un banco, una empresa de telecomunicaciones o una tienda en línea.
- Mensaje convincente: El mensaje generalmente incluye una declaración de urgencia o una oferta tentadora. Por ejemplo, puede informar a la víctima sobre una actividad inusual en su cuenta bancaria, un paquete que está en tránsito o un premio que ha ganado.
- Solicitud de acción inmediata: El mensaje insta a la víctima a tomar una acción inmediata, como hacer clic en un enlace o responder con información personal.
- Enlace malicioso: Si la víctima sigue el enlace proporcionado, será redirigida a un sitio web falso que simula ser la entidad legítima. En este sitio, se le pedirá que proporcione información personal o financiera.
- Recopilación de información: Una vez que la víctima proporciona la información solicitada, los atacantes la recopilan y pueden utilizarla para cometer fraudes financieros o robo de identidad.

Algunas de las estrategias comunes utilizadas en este tipo de estafa incluyen:

- Mensajes de alerta falsos: Los estafadores envían alertas fraudulentas sobre actividades sospechosas en cuentas bancarias o tarjetas de crédito, presionando a las víctimas para que verifiquen sus datos de inmediato.
- Promociones y premios falsos: Los destinatarios son informados de que han ganado un premio o sorteo, y se les pide que ingresen información personal o realicen un pequeño pago para reclamar su "premio".

- Suplantación de entidades oficiales: Se envían mensajes que aparentan ser de instituciones reconocidas, como la Sunat o el Banco de la Nación, solicitando datos personales para trámites supuestamente obligatorios.

De la misma forma, Diego Vences, experto en Data y Analytics de la empresa MoneyGram, explicó para este medio que “los SMS más comunes son aquellos que simulan emergencias o solicitudes de ayuda de familiares y amigos, intentando presionar a la víctima para que realice una transferencia de dinero. También son frecuentes los mensajes que suplantan a instituciones bancarias o que ofrecen empleos y premios falsos”.

"Las compañías deben hacer, no solo la evaluación correspondiente en sus procesos de seguridad, sino también que promuevan espacios de concientización para los consumidores", indicó.

Se deberían elevar medidas regulatorias como la promulgación de una ley que sancione tanto el smishing como el phishing en general, la obligación de que las empresas de telecomunicaciones implementen sistemas de seguridad capaces de detectar y bloquear mensajes fraudulentos antes de que lleguen a los usuarios, y la creación de programas educativos que fomenten la concientización.

El decano de la carrera de Ingeniería de Software de la Universidad Científica del Sur, Wester Zela, precisó, "El desarrollo de aplicaciones seguras frente a ataques de smishing presenta múltiples desafíos. Uno de los principales es la naturaleza dinámica y multifacética del smishing, que combina técnicas de explotación de vulnerabilidades y de ingeniería social, como la manipulación psicológica de los usuarios. Los desarrolladores deben construir sistemas que no solo puedan detectar y bloquear enlaces maliciosos, sino que también sean capaces de identificar patrones sospechosos de comportamiento que indiquen intentos de fraude. Esto requiere el uso de herramientas avanzadas, como la inteligencia artificial y el aprendizaje automático (machine learning), para mantenerse al día con las tácticas cambiantes de los atacantes".

“En segundo lugar, es recomendable utilizar la autenticación multifactorial (MFA), que añade una capa extra de seguridad y minimiza el riesgo de que un atacante que obtenga información a través de smishing pueda acceder a sistemas sensibles. Las actualizaciones regulares de software y sistemas también son esenciales para cerrar posibles vulnerabilidades. Finalmente, diseñar interfaces de usuario que incluyan advertencias claras sobre enlaces sospechosos puede ayudar a reducir el riesgo”, explicó.

3. RECOMENDACIONES:

- No hacer clic en enlaces sospechosos o no solicitados. En su lugar, visitar el sitio web escribiendo la dirección directamente en su navegador.
- Tener cuidado con las estafas telefónicas que podrían implicar la explotación de los datos robados.
- Practicar una higiene estricta de contraseñas. Utilizar contraseñas únicas para cada tarjeta y cambiarlas periódicamente.
- Habilitar la autenticación de dos factores cuando esté disponible.
- Mantener actualizados los sistemas operativos y aplicaciones de software.
- Guardar las evidencias y no eliminar los mensajes o correos electrónicos recibidos para facilitar el rastreo de los ciberdelincuentes, en caso hayan sido atacados y realicen la denuncia.
- Monitorear los movimientos de su cuenta bancaria afectada con el fin de detectar cargos no autorizados e informarlos a su entidad.
- Capacitar a los usuarios sobre las mejores prácticas de ciberseguridad.

Fuente de Información:	• hxxps://www.infobae.com/peru/2024/09/21/el-peligro-del-smishing-ciberdelincuentes-intensifican-el-uso-de-mensajes-sms-para-fraudes-en-peru/ • hxxps://www.infobae.com/peru/2024/05/06/aumentan-casos-de-smishing-en-el-peru-nueva-estafa-virtual-roba-datos-personales-desde-el-celular/ • hxxps://www.bancofalabella.pe/blog/smishing-que-es-ejemplos-como-evitarlo

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°249	Fecha: 28-10-2024 Página: 6 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de Omisión de funciones de seguridad en Okta Verify para iOS		
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 omisión de funciones de seguridad en Okta Verify para iOS. La explotación exitosa de esta vulnerabilidad podría permitir a un usuario autenticado remoto eludir la autenticación multifactor y obtener acceso no autorizado a la aplicación protegida con Okta Verify.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-10327 de tipo omisión de funciones de seguridad en Okta Verify para iOS, podría permitir a un atacante remoto eludir la autenticación multifactor.

La vulnerabilidad existe debido a que la aplicación permite respuestas de notificaciones push a través de la función ContextExtension de iOS, lo que hace que la víctima confirme la solicitud de autenticación independientemente de la opción seleccionada. Cuando un usuario mantiene presionado el banner de notificación y selecciona una opción, ambas opciones permiten que la autenticación sea exitosa. Un atacante remoto con conocimiento de la contraseña de la víctima (o con la capacidad de realizar un ataque de rociado de contraseñas) puede eludir la autenticación de segundo factor y obtener acceso no autorizado a la aplicación protegida con Okta Verify.

A. Productos afectados:

- Okta Verify para iOS: anteriores a la versión 9.27.2.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la versión 9.27.2 o posterior que aborda esta vulnerabilidad.
- Realizar una revisión exhaustiva del registro del sistema de Okta para identificar cualquier intento de autenticación no autorizado.
- Utilizar consultas de búsqueda específicas para comprobar si hay anomalías en el comportamiento del usuario en función de las direcciones IP y las geolocalizaciones.

Fuente de Información:	• hxxps://trust.okta.com/security-advisories/okta-verify-for-ios-cve-2024-10327 • hxxps://www.rescana.com/post/critical-vulnerability-in-okta-verify-for-ios-understanding-cve-2024-10327-and-mitigation-strategie • hxxps://cve.org/CVERecord?id=CVE-2024-10327

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°249	Fecha: 28-10-2024 Página: 7 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades en la configuración de F5 BIG-IP y las utilidades tmsh		
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:

F5 Networks ha publicado múltiples vulnerabilidades de severidad **MEDIA** de tipo agotamiento de los recursos y lectura fuera de límites en la configuración de F5 BIG-IP y las utilidades tmsh. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto no autenticado realizar un ataque de denegación de servicio (DoS) de la función que utiliza el componente afectado.

2. DETALLES:

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2019-1000020 de tipo agotamiento de los recursos y lectura fuera de límites en la configuración de F5 BIG-IP y las utilidades tmsh, podría permitir a un atacante remoto realizar un ataque de DoS. La vulnerabilidad existe debido a un análisis incorrecto de archivos ISO9660. Un atacante remoto puede persuadir a un usuario para que acceda a un archivo ISO9660, desencadenar una condición de bucle infinito y realizar un ataque de DoS.

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2019-1000019 de tipo lectura fuera de límites, podría permitir a un atacante remoto realizar un ataque de DoS. La vulnerabilidad existe debido a una condición de límite en la función header_bytes() en archive_read_support_format_7zip.c al descomprimir archivos 7zip. Un atacante remoto puede crear un archivo 7zip especialmente diseñado, engañar a la víctima para que lo abra, generar un error de lectura fuera de límites y bloquear la aplicación afectada.

A. Productos afectados:

- BIG-IP: 17.1.0 - 17.1.1.4, 17.0.0 - 17.0.0.2, 16.1.0 - 16.1.5, 16.0.0 - 16.0.1.2, 15.1.0 - 15.1.10.5, 15.0.0 - 15.0.1.4.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxp://my.f5.com/manage/s/article/K000148255 • hxxps://cve.org/CVERecord?id=CVE-2019-1000020 • hxxps://cve.org/CVERecord?id=CVE-2019-1000019

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°249	Fecha: 28-10-2024 Página: 8 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en el complemento WP Query Console 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 de código en el complemento WP Query Console de Lubus para WordPress. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante autenticado la inyección de código arbitrario, lo que podría provocar una ejecución remota de código en los sitios afectados.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2024-50498 de tipo inyección de código en WP Query Console para WordPress, podría permitir a un atacante la ejecución remota de código en el sitio web de destino. Esto se puede utilizar para obtener acceso por puerta trasera y luego tomar el control total del sitio web.

La vulnerabilidad permite a los usuarios autenticados inyectar código PHP arbitrario en el entorno de WordPress. Esto puede provocar una ejecución remota de código, donde los atacantes pueden ejecutar scripts maliciosos en el servidor y comprometer todo el sitio.

Los atacantes con los permisos suficientes pueden manipular la funcionalidad del complemento para ejecutar secuencias de comandos web arbitrarias, lo que puede comprometer la integridad y la seguridad del sitio de WordPress.

La presencia de esta vulnerabilidad aumenta la superficie de ataque general para los sitios de WordPress, especialmente aquellos con complementos obsoletos o medidas de seguridad insuficientes. Los atacantes pueden aprovechar esta vulnerabilidad como parte de campañas de explotación más amplias dirigidas a varios sitios.

A. Productos afectados:

- La vulnerabilidad afecta a todas las versiones del complemento LUBUS WP Query Console hasta la versión 1.0 inclusive.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.
- Revisar y actualizar periódicamente todos los complementos y temas para minimizar las vulnerabilidades.
- Implementar las mejores prácticas de seguridad, como el uso de firewalls de aplicaciones web (WAF) y el monitoreo de actividad inusual.
- Revisar los últimos avisos de seguridad e informes sobre posibles exploits que tengan como objetivo esta vulnerabilidad.

Fuente de Información:	• hxxps://patchstack.com/database/vulnerability/wp-query-console/wordpress-wp-query-console-plugin-1-0-remote-code-execution-rce-vulnerability • hxxp://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-50498

Índice alfabético