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

028-2025-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°028	Fecha: 03-02-2025
		Página: 4 de 11

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	La violación de datos de Globe Life podría afectar a 850.000 clientes más		
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:

Globe Life fue fundada en 1900 y es uno de los mayores proveedores de seguros de vida y salud de Estados Unidos. El 13 de junio de 2024, la compañía descubrió durante una revisión de seguridad de sus redes que había sido comprometida por piratas informáticos que habían obtenido acceso no autorizado a uno de sus portales web.

2. DETALLES:

La compañía ha compartido los últimos resultados de la investigación sobre la violación de datos en una nueva presentación ante la Comisión de Bolsa y Valores de Estados Unidos (SEC), y dice que el actor de la amenaza accedió a bases de datos específicas mantenidas por algunos propietarios de agencias independientes que tenían datos personales de aproximadamente 850.000 personas.

Los datos comprometidos, dice la compañía, pertenecen a clientes y prospectos de clientes, y probablemente fueron exfiltrados de su subsidiaria American Income Life Insurance Company.

La información potencialmente expuesta varía según el individuo y puede incluir:

- Nombres completos
- Direcciones de correo electrónico
- Números de teléfono
- Direcciones postales
- Fechas de nacimiento
- Números de Seguro Social (SSN)
- Datos relacionados con la salud
- Información de la póliza de seguro

Tras el incidente, el hacker se puso en contacto con la empresa para intentar extorsionarla. Sin embargo, Global Life afirma que se negó a pagar un rescate al atacante.

En respuesta, la empresa activó su plan de respuesta a incidentes y contrató expertos en ciberseguridad y asesores legales para investigar la violación.

La empresa se ha comprometido a proporcionar actualizaciones a medida que haya más información disponible y a cumplir con los requisitos reglamentarios.

3. RECOMENDACIONES:

- Permanecer atentos ante posibles intentos de phishing o robo de identidad utilizando los datos filtrados.
- No abrir enlaces recibidos por parte de contactos desconocidos
- Contactar directamente con la organización o empresa en cuestión para consultar el problema.
- No brindar información personal ni bancaria a través de plataformas digitales ni telefónicamente.
- Capacitar a los empleados sobre las mejores prácticas de ciberseguridad.

Fuente de Información:	• hxxps://gbhackers.com/globe-life-ransomware-attack/ • hxxps://www.securityweek.com/insurance-company-globe-life-notifying-850000-people-of-data-breach/ • hxxps://www.bleepingcomputer.com/news/security/globe-life-data-breach-may-impact-an-additional-850-000-clients/

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°028	Fecha: 03-02-2025
		Página: 5 de 11

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Aplicaciones que se deben eliminar de tu celular para proteger tu cuenta bancaria de un ciberataque		
Tipo de Ataque	Captura de información confidencial	Abreviatura	CIC
Medios de propagación	Red, Internet		
Código de familia	K	Código de Sub familia	K02
Clasificación temática familia	Uso inapropiado de recursos		

Descripción

1. ANTECEDENTES:

En medio de la creciente inseguridad y el avance de la era digital, los criminales virtuales representan una amenaza constante para los usuarios de internet. Con el auge de las transacciones en línea y el almacenamiento de información personal en dispositivos electrónicos, los ciberdelincuentes han desarrollado nuevas estrategias para acceder a datos sensibles.

2. DETALLES:

Uno de los métodos más utilizados en la actualidad es la distribución de aplicaciones maliciosas, diseñadas para recopilar información privada sin que la víctima lo note. A través de estos programas, los ciberdelincuentes pueden acceder a credenciales de acceso, historiales de navegación y datos bancarios, generando pérdidas económicas y suplantaciones de identidad.

Especialistas en ciberseguridad de la firma Kaspersky han alertado sobre la existencia de seis aplicaciones que, aunque aparentan ser servicios de Red Privada Virtual (VPN), en realidad operan con el objetivo de robar información personal y financiera de los usuarios.

- MaskVPN
- DewVPN
- PaladinVPN
- ProxyGate
- ShieldVPN
- ShineVPN

Estos programas han sido detectados actuando como herramientas para el robo de contraseñas, accesos bancarios y otros datos confidenciales, poniendo en riesgo la seguridad digital de quienes las instalan en sus dispositivos.

Al instalarse en un dispositivo móvil, estos programas funcionan como servidores proxy que interceptan la información que el usuario envía y recibe en línea. De esta manera, los ciberdelincuentes pueden recopilar credenciales bancarias, datos personales y registros de navegación sin que el afectado se percate de la actividad maliciosa.

Una vez que los atacantes obtienen información clave, pueden suplantar la identidad del usuario y realizar transacciones fraudulentas en su nombre.

Además, las falsas VPN pueden instalar otros tipos de malware en los dispositivos, lo que amplifica los riesgos de infección con virus, ransomware y otros programas dañinos.

Ahora existen mecanismos legales para denunciar estas vulneraciones y herramientas para proteger la información personal en el entorno digital.

Si tus datos han sido utilizados sin tu consentimiento o de manera indebida, puedes presentar una denuncia ante la **Autoridad Nacional de Protección de Datos Personales (ANPD)**, supervisada por el **Ministerio de Justicia y Derechos Humanos (MINJUSDH)**. Esta entidad puede sancionar a los responsables. Además, expertos en ciberseguridad han alertado sobre estas aplicaciones móviles que ponen en riesgo la seguridad de la información financiera de los usuarios.

Denunciar el uso indebido de datos personales es clave para **proteger la privacidad y evitar delitos** como el robo de identidad y el fraude financiero. La **ANPD** tiene la responsabilidad de fiscalizar y sancionar a quienes incumplen la **Ley 29733**, asegurando que las empresas y entidades estatales respeten la privacidad de los ciudadanos.

3. RECOMENDACIONES:

- Eliminar inmediatamente estas aplicaciones y optar por servicios de VPN confiables con políticas de privacidad claras.
- Verificar la autenticidad de las aplicaciones antes de descargarlas, revisando las reseñas, la empresa desarrolladora y los permisos que solicitan.
- Mantener actualizado el sistema operativo y las aplicaciones del dispositivo, para corregir vulnerabilidades de seguridad.
- Evitar redes Wi-Fi públicas para realizar operaciones bancarias o ingresar contraseñas.
- No compartir información personal en redes sociales ni en plataformas no seguras.
- Hacer uso de doble factor de autentificación siempre que sea posible.
- Utilizar contraseñas seguras y activar la autenticación en dos pasos en todas las cuentas sensibles, especialmente las bancarias.
- Evitar descargar aplicaciones desde fuentes desconocidas o enlaces sospechosos que puedan redirigir a programas fraudulentos.
- Instalar software de seguridad confiable, como antivirus y herramientas de detección de amenazas.
- Presentar una denuncia si considera que sus datos han sido utilizados de manera indebida. El proceso se puede realizar de dos formas:
  - **Virtual:** Completando el formulario de denuncia disponible en línea, adjuntando los documentos probatorios (capturas de pantalla, correos electrónicos o documentos que demuestren el uso indebido de los datos) y enviándolos a través del **Sistema de Gestión Documental (SGD)** o al correo protegetusdatos@minjus.gob.pe.
  - **Presencial:** Entregando el formulario impreso y los documentos en la **Mesa de Partes del MINJUSDH**, ubicada en **Calle Scipión Llona N.° 350, Miraflores**. El horario de atención es de lunes a viernes, de 8:00 a. m. a 4:30 p. m.
- Educar a los usuarios sobre las amenazas de ransomware y cómo reconocer los intentos de phishing, especialmente a los grupos más vulnerables, como los niños y adultos mayores.

Fuente de Información:	• hxxps://www.infobae.com/peru/2025/02/02/especialista-detallan-que-aplicaciones-debes-eliminar-de-tu-celular-para-proteger-tu-cuenta-bancaria-de-un-ciberataque/ • hxxps://www.infobae.com/peru/2025/02/02/denuncia-el-robo-de-tus-datos-personales-y-evita-ser-victima-de-ciberataques-desde-el-celular/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°028	Fecha: 03-02-2025 Página: 7 de 11

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidades de severidad crítica en productos Netgear		
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:

Netgear, Inc., ha publicado dos vulnerabilidades de severidad **CRÍTICA** de tipo omisión de autenticación que afectan a varios de sus modelos de routers y dispositivos. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto ejecutar comandos arbitrarios en los dispositivos afectados.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2024-12847 de tipo omisión de autenticación que afecta a varios modelos de routers y dispositivos, podría permitir a un atacante remoto no autenticado explotar una falla de omisión de autenticación, lo que permite ejecutar comandos arbitrarios del sistema operativo con privilegios de root mediante el envío de solicitudes HTTP especialmente diseñadas al punto final setup.cgi. Esta vulnerabilidad representa una amenaza significativa para los usuarios de enrutadores de NETGEAR DGN1000, lo que requiere una acción inmediata para proteger los dispositivos afectados y evitar el acceso no autorizado.

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2024-1430 de tipo divulgación de información que afecta a una funcionalidad desconocida del archivo “currentsetting.htm” del componente Web Management Interface, podría permitir que un atacante remoto no autenticado ejecute comandos arbitrarios en el dispositivo afectado. Esta vulnerabilidad representa un riesgo para los usuarios del enrutador Netgear R7000, y se recomienda aplicar medidas inmediatas para salvaguardar la información confidencial de posibles explotaciones.

A. Productos afectados:

- NETGEAR DGN1000: versiones de firmware anteriores a la 1.1.00.48.
- NETGEAR DGN2200 v1: todas las versiones (sin soporte actual).
- XR1000: versiones anteriores a 1.0.0.74.
- XR1000v2: versiones anteriores a 1.1.1.22.
- RBK852, RBR850, RBS850: versiones anteriores a 7.2.6.21.
- CAX30: versiones anteriores a 2.2.2.2.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de firmware disponibles que abordan estas vulnerabilidades.
- Actualizar el firmware del DGN1000 a la versión 1.1.00.48 o superior.
- Sustituir dispositivos antiguos que ya no reciben soporte, como el DGN2200 v1, se recomienda considerar su reemplazo por modelos más recientes y seguros.
- Implementar medidas de monitoreo para detectar actividades sospechosas en la red.
- Tomar medidas inmediatas para proteger sus redes y evitar compromisos de seguridad debido a estas vulnerabilidades críticas.

Fuente de Información:	• hxxps://kb.netgear.com/000066558/Security-Advisory-for-Unauthenticated-RCE-on-Some-WiFi-Routers-PSV-2023-0039 • hxxps://kb.netgear.com/000066557/Security-Advisory-for-Remote-Exploitation-on-Some-Wireless-Access-Points-PSV-2021-0117

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°028	Fecha: 03-02-2025 Página: 8 de 11

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en el complemento Metatagg Inc Custom 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:

Metatagg Inc. ha publicado una vulnerabilidad de severidad **ALTA** de tipo secuencias de comandos entre sitios (XSS) durante la generación de páginas web que afecta al complemento Metatagg Inc Custom para WordPress. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar código arbitrario e instalar un shell inverso en el sistema afectado.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-24676 de tipo secuencias de comandos entre sitios (XSS) durante la generación de páginas web que afecta al complemento Metatagg Inc Custom para WordPress. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar JavaScript arbitrario en el contexto del navegador de la víctima, lo que provocaría el secuestro de sesión, la redirección a sitios maliciosos u otras acciones maliciosas.

Esta vulnerabilidad afecta al complemento Metatagg Inc Custom que se utiliza en entornos WordPress. La principal preocupación es que implica una neutralización incorrecta de la entrada durante la generación de páginas web, lo que permite a un atacante inyectar secuencias de comandos maliciosas en páginas web vistas por otros usuarios.

Hasta el momento, no se conocen vulnerabilidades de explotación pública específicamente asociadas con esta vulnerabilidad de XSS que afecta al complemento Metatagg Inc Custom WP para WordPress.

A. Productos afectados:

- WordPress Custom WP Store Locator Plugin, versiones anteriores a 1.4.8.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad.
- Realizar validaciones de entrada estrictas para desinfectar las entradas de los usuarios y evitar que se ejecuten scripts maliciosos.
- Establecer políticas de seguridad de contenido (CSP) para restringir los orígenes desde los que se pueden cargar scripts.
- Realizar auditorías de seguridad periódicas y evaluaciones de vulnerabilidad en sus aplicaciones web para identificar y remediar posibles problemas de seguridad de forma proactiva.
- Concientizar a los usuarios sobre los riesgos asociados con XSS sobre temas de ciberamenazas.

Fuente de Información:	• hxxps://patchstack.com/database/wordpress/plugin/custom-store-locator/vulnerability/wordpress-custom-wp-store-locator-plugin-1-4-7-cross-site-scripting-xss-vulnerability

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°028	Fecha: 03-02-2025 Página: 9 de 11

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de Omisión de funciones de seguridad en productos AR		
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 identificadas en ciertas CPU basadas en ARM, en particular a varios procesadores Cortex-A y Neoverse. La explotación exitosa de esta vulnerabilidad podría permitir a un usuario autenticado remoto comprometer el hipervisor.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-5660 de tipo omisión de funciones de seguridad en productos ARM, podría permitir que un invitado malintencionado comprometa el hipervisor. La vulnerabilidad existe debido a una traducción incorrecta de la dirección de memoria cuando se habilita la agregación de páginas de hardware (HPA) y procesos relacionados, que pueden permitir que un sistema operativo invitado modificado y no confiable comprometa el sistema host cuando se ejecuta en un entorno de hipervisor.

La vulnerabilidad plantea un riesgo principalmente en entornos virtualizados donde los sistemas operativos invitados no confiables pueden explotar la falla para obtener acceso no autorizado o control sobre el sistema host. Esto podría provocar importantes brechas de seguridad si no se aborda con prontitud.

Hasta el momento, no hay pruebas de concepto públicas ni evidencia de explotación activa reportada. Sin embargo, los riesgos potenciales asociados con esta vulnerabilidad justifican la atención inmediata de los equipos de seguridad que administran los sistemas afectados.

A. Productos afectados:

- Cortex-A78: Todas las versiones.
- Cortex-A78C: Todas las versiones.
- Cortex-A78AE: Todas las versiones.
- Cortex-A710: Todas las versiones.
- Cortex-X1: Todas las versiones.
- Cortex-X1C: Todas las versiones.
- Cortex-X2: Todas las versiones.
- Cortex-X3: Todas las versiones.
- Cortex-X4: Todas las versiones.
- Cortex-X925: todas las versiones.
- Neoverse V1: Todas las versiones.
- Neoverse V2: Todas las versiones.
- Neoverse V3: Todas las versiones.
- Neoverse V3AE: Todas las versiones.
- Neoverse N2: Todas las versiones.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad.
- Deshabilitar la agregación de páginas configurando CPUECTLR_EL1[46] en 1.
- Monitorear las actualizaciones de Arm y otras fuentes relevantes para obtener parches o estrategias de mitigación a medida que estén disponibles.

Fuente de Información:	• hxxps://developer.arm.com/Arm%20Security%20Center/Arm%20CPU%20Vulnerability%20CVE-2024-5660

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°028	Fecha: 03-02-2025 Página: 10 de 11

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades en controladores de pantalla de GPU NVIDIA		
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:

NVIDIA Corporation ha publicado múltiples vulnerabilidades de severidad **ALTA** de tipo escritura fuera de límites, desbordamiento de búfer clásico, uso después de la liberación, limpieza incompleta y acceso al búfer con un valor de longitud incorrecto que afectan al controlador de pantalla GPU NVIDIA y el software vGPU, en sistemas Windows y Linux. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto no autenticado obtener acceso no autorizado a los archivos, generar una condición de denegación de servicio (DoS), manipular datos, divulgar información y la ejecución de código.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-0150 de tipo escritura fuera de límites en el controlador de pantalla de la GPU NVIDIA para Windows y Linux contiene una vulnerabilidad en la que los datos se escriben después del final o antes del comienzo de un búfer. Una explotación exitosa de esta vulnerabilidad podría provocar la divulgación de información, la denegación de servicio o la manipulación de datos.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-0146 de tipo desbordamiento de búfer clásico en el software NVIDIA vGPU contiene una vulnerabilidad en el Administrador de GPU virtual, donde un mal invitado podría provocar daños en la memoria. Una explotación exitosa de esta vulnerabilidad podría provocar la ejecución de código, la denegación de servicio, la divulgación de información o la manipulación de datos.

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2024-0147 de tipo uso después de la liberación en el controlador de pantalla de la GPU NVIDIA para Windows y Linux contiene una vulnerabilidad donde hacer referencia a la memoria después de haberla liberado puede provocar una denegación de servicio o manipulación de datos.

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2024-53869 de tipo limpieza incompleta en el controlador de memoria unificada NVIDIA para Linux contiene una vulnerabilidad que permite a un atacante filtrar memoria no inicializada. Si se explota esta vulnerabilidad con éxito, se podría divulgar información.

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2024-53881 de tipo limpieza incompleta en el software NVIDIA vGPU contiene una vulnerabilidad en el controlador del host, donde puede permitir que un invitado provoque una tormenta de interrupciones en el host, lo que puede provocar una denegación de servicio.

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2024-0131 de tipo acceso al búfer con un valor de longitud incorrecto controlador de núcleo de la GPU de NVIDIA para Windows y Linux contiene una vulnerabilidad que permite a un atacante en modo usuario leer un búfer con una longitud incorrecta. Una explotación exitosa de esta vulnerabilidad podría provocar una denegación de servicio.

Para la vulnerabilidad de severidad **baja** se ha asignado el siguiente identificador: CVE-2024-0149.

A. Productos afectados:

Estas vulnerabilidades afectan a una amplia gama de productos NVIDIA en diferentes ramas de controladores:

- Controladores de Windows: las GPU GeForce, NVIDIA RTX/Quadro/NVS y Tesla se ven afectadas en las ramas R535, R550, R560, R565 y R570. Las versiones actualizadas incluyen R535 (539.19), R550 (553.62) y R570 (572.16).
- Controladores de Linux: Problemas similares afectan a los controladores de Linux en las ramas R535, R550 y R570. Las versiones actualizadas incluyen R535 (535.230.02), R550 (550.144.03) y R570 (570.86.16).

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps://nvidia.custhelp.com/app/answers/detail/a_id/5614

Índice alfabético