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

031-2025-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°031	Fecha: 06-02-2025
		Página: 4 de 7

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Los actores de amenazas aprovechan el auge de DeepSeek para impulsar ciberataques		
Tipo de Ataque	Phishing	Abreviatura	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:

En los últimos días DeepSeek, la alternativa de China de código abierto a ChatGPT y otros LLM, ha logrado colocarse como la app más descargada en EE.UU., generando gran interés, pero despertando también algunas suspicacias, tanto por las campañas de phishing como por sus vulnerabilidades y la divulgación de información sensible, que lo ha llevado a ser prohibida en agencias gubernamentales centrales y locales de diferentes países.

2. DETALLES:

Luego del lanzamiento de DeepSeek, se detectó una campaña de distribución de malware a través de sitios falsos que imitan a la web oficial de esta herramienta de inteligencia artificial. En el sitio oficial, el botón principal dice "Start Now", ya que DeepSeek se usa directamente en la web. En el sitio falso, el botón dice "Download Now" y eso implica la descarga de un archivo malicioso. Si un usuario hace clic en el botón del sitio falso, se descarga un archivo ejecutable (.exe) con el nombre de DeepSeek.

Se descubrió también que los modelos de IA de DeepSeek son susceptibles a ataques adversarios, incluidos los “jailbreaks malvados”. Los jailbreaks de IA explotan las debilidades en las restricciones de un modelo para eludir los controles de seguridad y obtener respuestas no autorizadas.

Los jailbreaks permiten a los atacantes eludir restricciones y generar contenido no censurado o dañino. Se ha identificado casos en los que estos modelos se utilizaron para desarrollar malware destinado a robar información y extraer información confidencial de usuarios desprevenidos, o eludir las protecciones antifraude bancarias, lo que potencialmente permite un robo financiero a gran escala.

Hablando de su política de privacidad, DeepSeek indica que recopila información personal tanto del perfil como de la información que comparte el usuario con la IA, incluso información procedente del dispositivo desde donde el usuario use la aplicación. Por ello, DeepSeek ha sido objeto de críticas por cuestiones de privacidad y seguridad.

La fuga de información de DeepSeek pone de relieve problemas críticos en la industria de la IA: fallas de seguridad, gobernanza de datos y responsabilidad ética.

Por ejemplo, la aplicación transmite datos confidenciales del usuario sin cifrar, lo que la deja vulnerable a la interceptación. Además, estos datos son enviados a servidores controlados por ByteDance bajo jurisdicción china, lo que genera inquietudes, pues podría poner en peligro la seguridad de la información nacional. Por ello, en varios países se estableció su prohibición.

3. RECOMENDACIONES:

- Desinstalar la aplicación y restablecer las credenciales utilizadas en ella.
- Evitar correos mensajes no solicitados que promocionen ofertas relacionadas con DeepSeek.
- Verificar la URL antes de acceder o ingresar datos.
- No ingresar información confidencial en los sistemas de IA sin realizar evaluaciones de riesgos adecuadas.
- Consultar fuentes confiables para conocer posibles riesgos y campañas activas.
- Usar soluciones de seguridad para analizar archivos antes de ejecutarlos.

Fuente de Información:	• hxxps://gbhackers.com/deepseeks-new-jailbreak-method/ • hxxps://gbhackers.com/threat-actors-exploiting-deepseeks-rise/ • hxxps://www.welivesecurity.com/es/estafas-enganos/deepseek-ai-utilizado-malware-sitios-falsos/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°031	Fecha: 06-02-2025
		Página: 5 de 7

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad media en comandos SQL ERP-ONE+ VeraCore de Advantive		
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:

Advantive ha publicado una vulnerabilidad de severidad **MEDIA** de tipo neutralización incorrecta de elementos especiales utilizados en un comando SQL (*SQL Injection*), que afecta a versiones hasta 2025.1.0 de ERP-ONE+ VeraCore. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autorizado ingresar a la base de datos, Dado que las bases de datos SQL generalmente contienen datos confidenciales, la pérdida de confidencialidad es un problema frecuente con las vulnerabilidades de inyección SQL.

2. DETALLES:

La vulnerabilidad de severidad **MEDIA** identificada por MITRE como CVE-2025-25181 de tipo neutralización incorrecta de elementos especiales utilizados en un comando SQL, que afecta a versiones hasta 2025.1.0 de VeraCore, podría permitir a un atacante remoto ejecutar comandos SQL arbitrarios a través del parámetro "PmSess1" en timeoutWarning.asp, en la base de datos de la aplicación, lo que puede resultar en el robo de credenciales, la ejecución remota de código y el acceso persistente a sistemas comprometidos. Así como puede ser posible leer información confidencial, también es posible modificar o incluso eliminar esta información con un ataque de inyección SQL.

Esta vulnerabilidad se puede encontrar dentro de la categoría A03:2021 – Inyección en el OWASPT Top 10.

A. Análisis Técnico:

Es una vulnerabilidad de inyección SQL identificada en la aplicación VeraCore, específicamente dentro del punto final timeoutWarning. Este error surge porque la aplicación construye consultas SQL concatenando un parámetro proporcionado por el usuario (PmSess1) directamente en la cadena de consulta sin la desinfección adecuada. En consecuencia, un atacante puede manipular el parámetro PmSess1 para ejecutar comandos SQL arbitrarios en la base de datos de la aplicación.

B. Calificaciones:

- De fácil divulgación.
- No autenticado.
- Vulnerable en la configuración predeterminada.

C. Productos afectados:

- VeraCore ERP-ONE+ hasta la versión 2025.1.0.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad.
- Ejecutar su código utilizando los privilegios más bajos que se requieren para realizar las tareas necesarias.
- Utilizar LIMIT y otros controles SQL dentro de las consultas para evitar la divulgación masiva de registros en caso de inyección SQL.
- Utilizar herramientas y técnicas dinámicas que interactúen con el software utilizando grandes conjuntos de pruebas con entradas diversas, como prueba de *fuzzing*, pruebas de robustez e inyección de errores.
- Desactivar todas las opciones que hagan que los mensajes de error de la base de datos se devuelvan al usuario. Advantive ha desactivado temporalmente la función de carga vulnerable, actualmente no hay parche disponible.

Fuente de Información:	• hxxps[:]//advantive[.]my[.]site[.]com/support/s/article/ERP-ONE-Version-2025-1-2-Release -Notes • hxxps[:]//cwe[.]mitre[.]org/data/definitions/89[.]html • hxxps[:]//attackerkb[.]com/topics/XqkJhTdX8Y/cve-2025-25181

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°031	Fecha: 06-02-2025 Página: 6 de 7

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en aplicación de DumbDrop		
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:

DumbWareio ha publicado vulnerabilidades de severidad **CRÍTICA** de tipo: Neutralización inadecuada de elementos especiales utilizados en un comando del Sistema Operativo "*Inyección de comando del SO*", que afecta a la aplicación de carga de archivos *DumbDrop*. La explotación exitosa de esta vulnerabilidad posibilitaría a un atacante a ejecutar código arbitrario de forma remota cuando "*Apprise*" servicio de notificaciones esté habilitado.

2. DETALLES:

La vulnerabilidad de severidad **CRITICA** identificada por MITRE como CVE-2025-24971, que afecta a la aplicación de carga de archivos *DumbDrop*, específicamente al punto terminal (*Endpoint*) POST **/upload/init**, permitiendo que un atacante ejecute código arbitrario de forma remota cuando "*Apprise*" servicio de notificaciones esté habilitado. Dado que no hay validación de la entrada del lado del usuario, es posible la inyección de comandos del sistema operativo.

Este problema se ha solucionado en la confirmación "4ff8469d" y se recomienda a todos los usuarios que apliquen el parche. No se conocen soluciones alternativas para esta vulnerabilidad.

Esta vulnerabilidad se puede encontrar dentro de la categoría A03:2021 – Inyección en el OWASPT Top 10.

A. Impacto:

- Un atacante puede obtener información directamente del sistema y usarla en un ataque secundario.
- Si un atacante obtiene privilegios de "root" a través de un ataque de elevación de privilegios, puede tomar el control de un servidor web e instalar malware.
- Ejecuta malware de criptominería o criptojacking que utiliza los recursos informáticos de un dispositivo infectado para extraer criptomonedas, para el beneficio financiero del atacante.

B. Calificaciones:

- In the wild.

C. Productos afectados:

- DumbDrop (Docker) todas las versiones commit 4ff8469d.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad.
- Comprobar el hash de confirmación de tu instalación de DumbDrop, si es anterior a 4ff8469d, la instancia es vulnerable.
- Descargar la última versión desde el repositorio o sitio web oficial de DumbDrop.

Fuente de Información:	• hxxps://github.com/DumbWareio/DumbDrop/security/advisories/GHSA-rx8m-jqm7-vcgp

Índice alfabético