GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °2626

BOLETÍN DE CIBERSEGURIDAD SEMANAL

Bienvenido a su boletín semanal de ciberseguridad generado por Gamma Ingenieros. A través de esta publicación tenemos el propósito de compartir contenidos relevantes para nuestras operaciones y aliados de negocio.

Aquí encontrará información sobre vulnerabilidades, alertas tempranas, noticias del sector, incidentes de ciberseguridad, tecnologías y servicios relacionados, entre otros.

VISTA RÁPIDA

	CRÍTICO	URGENTE	IMPORTANTE
VULNERABILIDADES	2	1	0
MALWARE	0	1	0
NOTICIAS DE CIBERSEGURIDAD	0	1	0

VULNERABILIDADES

CVE-2026-8037 – PROGRESS KEMP LOADMASTER (EJECUCIÓN REMOTA DE CÓDIGO PRE-AUTENTICACIÓN)

Se ha identificado la explotación activa en entornos reales de una vulnerabilidad crítica de inyección de comandos que afecta al balanceador de carga y controlador de entrega de aplicaciones (ADC) Progress Kemp LoadMaster. Al estar posicionado habitualmente en el perímetro de la red, este fallo permite a actores de amenazas remotos y no autenticados ejecutar comandos arbitrarios con privilegios elevados directamente en el dispositivo a través de solicitudes maliciosas dirigidas a la interfaz de su API.

Resumen técnico:

- Identificador principal: CVE-2026-8037 (ID alternativo: ZDI-26-342).
- Severidad: Crítica (Puntaje base de 9.8 en CVSS v3.0 / 9.6 en CVSS v4.0).
- Causa raíz: Una falla de sanitización y manejo incorrecto de memoria dinámica (heap) dentro de la función interna escape_quotes() en el ejecutable de acceso. La función asigna memoria desinicializada mediante malloc() y no añade un terminador nulo (\0) al final de la cadena de caracteres procesada.
- Mecanismo de falla: El fallo es explotable a través del endpoint /accessv2 cuando la interfaz API se encuentra habilitada. Un atacante realiza un ataque de inundación de memoria (heap spraying) enviando múltiples parámetros JSON clave-valor con una carga útil maliciosa adyacente a la variable apiuser. Al enviar cuatro comillas simples ("") en dicho parámetro, la expansión genera 16 bytes que sobrescriben los metadatos del bloque de memoria contiguo, eliminando los bytes nulos de control y forzando a la función sprintf / system() a leer y ejecutar la carga útil inyectada en la shell del sistema operativo.
- Estado de explotación: Explotación activa confirmada en la naturaleza a partir del 29 de junio de 2026. Los detalles técnicos profundos y el código de prueba de concepto (PoC) funcional fueron publicados de forma abierta en la misma fecha por laboratorios de investigación (watchTowr Labs), acelerando los barridos de escaneo automatizados.
- Versiones afectadas: Progress Kemp LoadMaster en ramas de lanzamiento general (GA) versiones 7.2.63.1 y anteriores; ramas de soporte a largo plazo (LTSF) versiones 7.2.54.17 y anteriores. El fallo también se extiende a los componentes Progress ECS Connection Manager y Progress Connection Manager para ObjectScale.

Impacto potencial:

- Ejecución de código arbitrario con máximos privilegios (Root): La explotación exitosa concede al atacante la capacidad de ejecutar comandos del sistema directamente en la consola del appliance con el nivel de superusuario, comprometiendo por completo la integridad de la máquina.
- Punto de entrada perimetral y movimiento lateral desobstruido: Debido a que estos dispositivos operan en el límite perimetral (DMZ) y poseen visibilidad hacia servicios y redes internas críticas, un servidor comprometido sirve como el pivote perfecto para realizar escaneos internos y ataques hacia el Directorio Activo u otros repositorios de credenciales.
- Interceptación y exfiltración de tráfico confidencial: Al controlar el balanceador de carga, el atacante se posiciona de forma privilegiada para interceptar, descifrar o desviar el tráfico de red legítimo de las aplicaciones empresariales protegidas, incluyendo cookies de sesión, datos personales y tokens de autenticación (gracias al SSL/TLS offloading).
- Interrupción total del negocio y desactivación del WAF: Los atacantes pueden desconfigurar las políticas de distribución de carga, deshabilitar las reglas del Web Application Firewall (WAF) integrado o interrumpir por completo la disponibilidad de los portales web legítimos expuestos a internet, provocando una denegación de servicio (DoS) sostenida.

Recomendaciones de mitigación:

1. Actualización inmediata de firmware a versiones seguras: Se urge a los administradores a aplicar de forma prioritaria las actualizaciones oficiales provistas por el fabricante, migrando los entornos afectados hacia Kemp LoadMaster GA v7.2.63.2 o LTSF v7.2.54.18 (o las versiones corregidas homólogas en entornos ECS y ObjectScale).
2. Restricción perimetral de la API mediante políticas de red: En caso de no poder aplicar el parche de manera inmediata, se debe limitar estrictamente el acceso al endpoint /accessv2. Configure listas de control de acceso (ACL) y firewalls para permitir el tráfico hacia la API únicamente desde segmentos de red de gestión internos aislados o direcciones IP de administración explícitamente confiables.
3. Búsqueda activa de Indicadores de Compromiso (Threat Hunting): Auditar de forma exhaustiva los logs del balanceador y las soluciones de monitoreo perimetral en busca de peticiones JSON inusualmente largas o anómalas dirigidas a /accessv2. Adicionalmente, valide el bloqueo preventivo en sus soluciones de seguridad de las IPs atacantes reportadas en las campañas iniciales: 192.42.116.58, 192.42.116.105 y 146.70.139.154.
4. Deshabilitación temporal de la interfaz API: Si los flujos operacionales e integraciones de la infraestructura de la organización no requieren el uso automatizado de la API de administración de LoadMaster, se recomienda proceder con su desactivación total en el panel de control del dispositivo para remover por completo la superficie de ataque expuesta.

Prioridad: Crítica.

Ampliar información:

- https://cybersecuritynews.com/critical-progress-kemp-loadmaster-vulnerability/
- https://www.scworld.com/brief/progress-kemp-loadmaster-vulnerability-actively-exploited
- https://labs.watchtowr.com/enterprise-tech-in-shell-out-progress-kemp-loadmaster-uninitialized-heap-to-pre-auth-rce-cve-2026-8037/
- https://thehackernews.com/2026/07/latest-progress-kemp-loadmaster-pre.html
- https://www.esentire.com/security-advisories/progress-kemp-loadmaster-vulnerability-targeted-cve-2026-8037
- https://vpncentral.com/critical-progress-kemp-loadmaster-flaw-allows-pre-auth-root-command-execution/

Citrix NetScaler ADC / Gateway – CVE-2026-8451, CVE-2026-8452, CVE-2026-8655, CVE-2026-10816, CVE-2026-10817 y CVE-2026-13474

Se han divulgado de forma oficial seis vulnerabilidades en los appliances perimetrales NetScaler ADC y NetScaler Gateway. Estos fallos de seguridad permiten a actores de amenazas realizar la lectura no autenticada de archivos locales del sistema, provocar la fuga de información sensible residente en la memoria dinámica mediante solicitudes malformadas o generar condiciones severas de Denegación de Servicio (DoS). Debido al rol crítico que juegan estos dispositivos en la autenticación, balanceo y terminación de sesiones VPN, su corrección expone una urgencia operativa alta para evitar vectores de compromiso inicial.

Resumen técnico:

- Identificador principal: CVE-2026-8451, CVE-2026-8452, CVE-2026-8655, CVE-2026-10816, CVE-2026-10817 y CVE-2026-13474 (Boletín de seguridad CTX696604).
- Severidad: Alta (Puntajes base de CVSS v4.0 que oscilan entre 6.9 y 8.8, dependiendo del vector específico).
- **Causa raíz:** Vulnerabilidades derivadas de una gestión deficiente de memoria, validación insuficiente de entradas XML/SAML, controles inadecuados sobre rutas de archivos y fallas en la liberación de memoria durante conexiones HTTP/2.
- Mecanismo de falla: El comportamiento varía según las características activadas en el appliance:
- En SAML IdP (CVE-2026-8451), el procesamiento de solicitudes estructuradas incorrectamente en /saml/login confunde las fronteras del parser XML, provocando una sobre-lectura de búfer que inyecta datos huérfanos de la memoria en la cookie de respuesta NSC_TASS.
- En Interfaces de Gestión (CVE-2026-10816), la falta de sanitización de rutas permite la descarga remota de archivos arbitrarios si se accede a las IPs de administración (NSIP, Cluster Management IP o SNIP habilitadas).
- En HTTP/2 y Perfiles TCP (CVE-2026-13474 y CVE-2026-10817), el envío de tramas malformadas colapsa o fuga recursos de red del proceso core nsppe.
- **Estado de explotación:** A la fecha del boletín (30 de junio de 2026) no existe evidencia de explotación activa. No obstante, la publicación de análisis técnicos detallados por parte de investigadores aumenta el riesgo de campañas de escaneo y posibles ataques en el corto plazo.
- Versiones afectadas: Ramas de soporte comercial NetScaler ADC y NetScaler Gateway 14.1 anteriores a la compilación 14.1-72.61; y versiones de la rama 13.1 anteriores a 13.1-63.18. El fallo impacta de igual manera a los firmwares basados en estándares de cumplimiento normativo FIPS (ramas 14.1 y 13.1), NDcPP y arquitecturas híbridas de Secure Private Access.

Impacto potencial:

- Exfiltración de credenciales, secretos e información de identidad: El fallo de lectura de archivos y la fuga de memoria en el módulo SAML facultan a los atacantes para extraer archivos internos de configuración, llaves criptográficas de certificados, tokens de sesión o metadatos de federación empresarial, lo que debilita el límite de confianza de la identidad corporativa.
- Denegación de Servicio (DoS) e interrupción total del acceso remoto: La explotación de los desbordamientos de búfer en pasarelas SSL VPN, servidores virtuales AAA, proxies DNS o balanceadores de bases de datos Oracle puede provocar caídas repetitivas y bloqueos severos del proceso central de procesamiento de paquetes (nsppe), interrumpiendo el flujo operativo de los empleados remotos y la disponibilidad de los servicios publicados.
- Secuestro de flujos de autenticación e integraciones Single Sign-On (SSO): Al explotar el fallo de lectura fuera de límites en el rol de proveedor de identidad (SAML IdP), los atacantes pueden recolectar datos estructurados de otras sesiones de usuario concurrentes, facilitando potenciales ataques dirigidos de bypass de autenticación o manipulación de respuestas de redirección.
- Facilitación de movimientos laterales y reconocimiento de red interna: Si las interfaces de gestión del dispositivo se encuentran expuestas o son alcanzables por un atacante con acceso inicial básico en la red, la extracción no autorizada de logs de auditoría y tablas de rutas internas a través de la lectura arbitraria de archivos acelerará el mapeo de activos de alto valor dentro de la infraestructura.

Recomendaciones de mitigación:

1. Actualización prioritaria a firmwares estables y corregidos: Cloud Software Group insta firmemente a desplegar los parches de seguridad de forma inmediata migrando a las versiones NetScaler 14.1-72.61 o 13.1-63.18 (o las compilaciones correspondientes según su subtipo FIPS / NDcPP).
2. Aplicación del ajuste obligatorio de mitigación para HTTP/2 (CVE-2026-13474): Si su organización no utiliza un perfil estricto de HTTP (HTTP Strict Profile), la simple actualización de firmware no solucionará por completo la vulnerabilidad de denegación de servicio. Es mandatorio configurar manualmente el nuevo parámetro Http2SmallWndTimeout a un valor recomendado de 30 segundos en todos sus perfiles HTTP activos mediante el comando: set ns httpProfile <nombre_perfil> -http2SmallWndTimeout 30
3. Restricción absoluta y endurecimiento del plano de control/administración: Asegure que los accesos de gestión a través de las direcciones IP de administración de NetScaler (NSIP, Cluster Management IP o Subnet IP - SNIP con acceso administrativo habilitado) estén estrictamente aislados de redes externas o de zonas de usuarios comunes. Deben restringirse únicamente a segmentos de administración dedicados (VLAN de gestión) protegidos por firewalls perimetrales y mecanismos robustos de control de acceso.
4. Auditoría de configuración orientada a condiciones previas (Triage rápido): Ejecute revisiones proactivas sobre el archivo de configuración consolidado (/nsconfig/ns.conf) buscando las directivas que activan los vectores expuestos: verifique la existencia de perfiles SAML activos (add authentication samlIdPProfile), servidores de autenticación virtuales (add authentication vserver), servidores virtuales de tipo Oracle/DNS o perfiles TCP heredados con la opción TimeStamp ENABLED para priorizar los activos con mayor nivel de exposición.

Prioridad: Urgente.

Ampliar información:

- https://vulert.com/blog/citrix-netscaler-six-flaws-file-read-dos/
- https://www.penligent.ai/hackinglabs/es/cve-2026-8451/
- https://www.kraftkennedy.com/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve-2026-8451-cve-2026-8452-cve-2026-8655-cve-2026-10816-cve-2026-10817-and-cve-2026-13474/
- https://thehackernews.com/2026/07/citrix-patches-six-netscaler-flaws.html
- https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696604

CVE-2026-48276, CVE-2026-48277, CVE-2026-48281, CVE-2026-48282 y CVE-2026-48283 – ADOBE COLDFUSION (EJECUCIÓN REMOTA DE CÓDIGO Y MÚLTIPLES IMPACTOS CRÍTICOS)

Adobe ha publicado un boletín de seguridad extraordinario de Prioridad 1 para resolver un conjunto masivo de vulnerabilidades críticas que afectan a su plataforma de desarrollo de aplicaciones web Adobe ColdFusion. Seis de estos fallos han recibido la calificación máxima de severidad (CVSS 10.0) debido a que permiten la ejecución remota de código (RCE) por parte de atacantes de red no autenticados. La explotación exitosa de este conjunto de fallas expone a los servidores de aplicaciones a un compromiso total, permitiendo el despliegue de web shells y la desactivación de controles perimetrales.

Resumen técnico:

- Identificador principal: CVE-2026-48276, CVE-2026-48277, CVE-2026-48281, CVE-2026-48282 y CVE-2026-48283 (Boletín oficial de seguridad APSB26-68).
- Severidad: Crítica (Seis fallas con el puntaje máximo de 10.0 en la escala CVSS v3.1; fallas asociadas de 9.3 y 8.8).
- Causa raíz: Debilidades graves asociadas a la subida irrestricta de archivos con tipos peligrosos (CWE-434), fallas generalizadas en la validación de parámetros de entrada (CWE-20), y deficiencias en la limitación de nombres de ruta hacia directorios restringidos o salto de directorio (CWE-22 / Path Traversal).
- Mecanismo de falla: A través de vectores independientes expuestos en la red, un atacante remoto no autenticado puede estructurar peticiones HTTP maliciosas hacia el motor de ColdFusion. Esto le permite evadir las restricciones de carga de extensiones web para inyectar scripts maliciosos (por ejemplo, archivos .cfm o .jsp) en rutas públicas del servidor web, o manipular variables de ruta para forzar al backend a procesar u otorgar salida a archivos confidenciales del sistema operativo mediante técnicas de deserialización insegura o sobreescritura.
- Estado de explotación: No se han confirmado ataques activos en entornos de producción al momento de la emisión del parche (30 de junio de 2026). Sin embargo, el fabricante ha catalogado el boletín con la clasificación de Prioridad 1 (máxima urgencia operativa) y ha anunciado la aceleración de sus ciclos de actualización debido a que el uso de modelos de Inteligencia Artificial Avanzada está reduciendo la brecha entre la publicación de la vulnerabilidad y la ingeniería inversa para la creación de exploits funcionales de días a pocas horas.
- Versiones afectadas: Adobe ColdFusion 2025 en sus versiones de Actualización 9 (Update 9) y anteriores; y Adobe ColdFusion 2023 en sus versiones de Actualización 20 (Update 20) y anteriores, bajo todas las plataformas operativas soportadas.

Impacto potencial:

- Ejecución de comandos arbitrarios en el servidor (RCE): Al abusar de las fallas de subida de archivos y Path Traversal de impacto 10.0, un atacante puede tomar el control operativo completo del servidor web subyacente, ejecutando utilidades del sistema en el contexto del servicio de ColdFusion.
- Fuga masiva de datos y lectura arbitraria de archivos locales: Mediante el fallo de Path Traversal complementario (CVE-2026-48313, CVSS 9.3), los actores de amenazas pueden descargar archivos críticos del sistema operativo, códigos fuente de aplicaciones empresariales, cadenas de conexión a bases de datos y archivos de configuración que contengan llaves criptográficas o credenciales en texto plano.
- Bypass de características de seguridad y pivoteo interno (SSRF): La existencia de una vulnerabilidad de falsificación de solicitud del lado del servidor (SSRF - CVE-2026-48285) faculta a los atacantes para usar la confianza del servidor expuesto a internet para escanear la red interna, atacar APIs privadas e interactuar con servicios locales que no deberían tener exposición perimetral.
- Escalada de privilegios y persistencia de amenazas: El encadenamiento de fallas de validación de entrada e inyección de scripts reflected (XSS) permite a atacantes de baja jerarquía heredar privilegios de administración o forzar a administradores legítimos a ejecutar acciones maliciosas en el backend de gestión, facilitando la instalación de puertas traseras (backdoors) persistentes.

Recomendaciones de mitigación:

1. Actualización prioritaria e inmediata a versiones seguras: Se exhorta a los equipos de infraestructura y administración de aplicaciones a desplegar de forma urgente los parches oficiales de Adobe, migrando los entornos ColdFusion 2025 hacia el Update 10 y los entornos ColdFusion 2023 hacia el Update 21.
2. Configuración estricta del filtro de serialización de Java (JVM): Implemente y aplique de forma estricta las directivas del filtro serial centralizado de ColdFusion agregando la opción -Djdk.serialFilter=... en los argumentos de inicio de la máquina virtual de Java (JVM), bloqueando activamente el procesamiento de objetos binarios no autorizados que facilitan ataques de deserialización.
3. Actualización del conector JDBC y mitigación de base de datos: Como medida de seguridad complementaria recomendada explícitamente por el fabricante para este ciclo de seguridad, actualice el conector Java de MySQL (MySQL Java Connector) a su última versión estable para prevenir vectores colaterales de inyección y manipulación de datos.
4. Aislamiento perimetral y aplicación de la Guía de Bloqueo (Lockdown Guide): Restrinja por completo el acceso externo directo a los puertos e interfaces administrativas del portal de ColdFusion (como /CFIDE/administrator). Adicionalmente, ejecute una auditoría completa de endurecimiento siguiendo los lineamientos de la guía oficial de aseguramiento (ColdFusion Lockdown Guide) para asegurar la ejecución del servicio bajo el Principio de Menor Privilegio (cuenta de usuario local sin derechos administrativos).

Prioridad: Crítica.

Ampliar información:

- https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-adobe-products-could-allow-for-arbitrary-code-execution_2026-066
- https://www.securityweek.com/adobe-patches-critical-coldfusion-campaign-classic-vulnerabilities/
- https://threatprotect.qualys.com/2026/07/01/adobe-releases-patches-for-coldfusion-critical-vulnerabilities/
- https://socradar.io/blog/adobe-coldfusion-campaign-classic-rce-flaws/?__cf_chl_f_tk=KYDQxKfI38uVs5HdFWTz.9V4sLJ58g8fsPiHtZSmO4Y-1782965811-1.0.1.1-coi2P425x4k2bKsIFW.tG.bvB83VzS34Lh8XQxpdOXU
- https://cybersecuritynews.com/multiple-adobe-coldfusion-vulnerabilities/
- https://thehackernews.com/2026/07/adobe-patches-7-cvss-100-flaws-in.html
- https://helpx.adobe.com/uk/security/products/coldfusion/apsb26-68.html

MALWARE

OUSABAN BANKING TROJAN – TROYANO BANCARIO GEOLOCALIZADO (ROBO DE CREDENCIALES Y SECUESTRO DE SESIÓN)

Se ha detectado una campaña dirigida y altamente evasiva del troyano bancario Ousaban (también conocido como Javali) dirigida específicamente contra usuarios de entidades financieras en la península ibérica (España y Portugal). Este malware, de origen brasileño y perteneciente al grupo histórico de amenazas conocido como "La Tétrade", ha sido actualizado con capacidades avanzadas de evasión que incluyen técnicas de geofencing del lado del servidor, esteganografía para ocultar sus cargas útiles dentro de imágenes inocuas y un sistema de generación de dominios dinámicos (DGA) diario para dificultar el bloqueo preventivo de sus servidores de comando y control (C2).

Resumen técnico:

- Identificador principal: Ousaban Banking Trojan (Alias: Javali).
- Severidad: Alta.
- Causa raíz: Ejecutable malicioso basado en Windows (desarrollado tradicionalmente en Delphi) que utiliza inyección de procesos y técnicas de secuestro de carga de librerías (DLL Side-Loading) para evadir las soluciones tradicionales de detección en el endpoint.
- Mecanismo de propagación: La infección comienza con un correo de phishing que contiene un archivo PDF malicioso simulando estar dañado. El documento incita a la víctima a hacer clic en un botón de "Actualizar" (Atualizar) o ejecuta código JavaScript embebido y ofuscado en hexadecimal de manera autónoma. Esto redirige al usuario a un sitio web fraudulento que simula ser un portal de impuestos gubernamentales. Dicha página realiza una exhaustiva validación del entorno (geofencing por IP, idioma, zona horaria y descarte de conexiones VPN o sandboxes de análisis). Si el entorno es apto, descarga un archivo VBScript que utiliza esteganografía para bajar una imagen con apariencia de icono de PDF que tiene un contenedor ZIP oculto en su estructura binaria. El script extrae el troyano final, lo aloja en la ruta C:\SysMain_5874288 y elimina los artefactos descargados para borrar su rastro.
- Mecanismo de Comando y Control (C2): Ousaban cuenta con un diseño de infraestructura evasiva. Utiliza una publicación señuelo en Pastebin que apunta a una IP privada muerta con el fin de desviar la atención de los analistas de seguridad. El canal real con el C2 se establece mediante un algoritmo de generación de dominios (DGA) que cambia diariamente. Para calcular el dominio del día, el malware consulta legítimamente una página de Google para extraer la fecha exacta actual, la combina con una cadena secreta hardcodeada en su código y genera un hash MD5 que actúa como subdominio de un servicio de DNS dinámico (DDNS).

Impacto potencial:

- Monitoreo activo y robo de credenciales: El troyano permanece latente en el sistema operativo hasta que detecta que el usuario accede a través del navegador web a alguno de los portales financieros objetivo. En ese momento, activa módulos de captura de pulsaciones de teclado (keylogging) para robar contraseñas en texto plano.
- Secuestro y control remoto de sesiones bancarias: A través del comando enviado desde el C2 conocido como #Iniciar#, los atacantes adquieren la capacidad de controlar de forma remota el mouse, el teclado y realizar capturas de pantalla en tiempo real de la máquina de la víctima, permitiéndoles realizar transferencias no autorizadas directamente sobre una sesión web legítima y evadir los controles de doble factor de autenticación (MFA).
- Inyección y manipulación del portapapeles: El malware cuenta con la función de monitorear y alterar la información copiada en el portapapeles del sistema operativo (clipboard injection). Esto le permite sustituir de manera silenciosa números de cuenta destino (como códigos IBAN) o direcciones de billeteras de criptomonedas por billeteras controladas por la estructura criminal al momento de realizar transacciones.
- Despliegue de pantallas emergentes fraudulentas: Para inducir al error al operador de la máquina, Ousaban puede superponer ventanas y formularios falsos idénticos a los de las bancas legítimas, solicitando al usuario códigos de verificación dinámicos, tokens o datos confidenciales complementarios para entregárselos directamente al atacante en su panel operativo.

Recomendaciones de mitigación:

1. Bloqueo inmediato de Indicadores de Compromiso (IoCs): Implementar reglas de restricción perimetral en firewalls y sistemas de filtrado web para bloquear el acceso hacia los dominios identificados en la campaña (faturanova.xyz, facture-in.pages.dev, controlfacturas.site) así como las direcciones IP de los servidores identificados por los sensores de amenazas.
2. Monitoreo de persistencia y auditoría de registros: Configurar firmas de búsqueda en soluciones EDR/SIEM para identificar la creación de valores anómalos en el registro de Windows, específicamente el valor denominado Financeiro dentro de la clave de ejecución automática CurrentVersion\Run, así como la creación de carpetas o ejecutables sospechosos bajo la ruta local C:\SysMain_5874288.
3. Robustecimiento de las políticas del Gateway de Correo (SEG): Configurar reglas estrictas de inspección en las soluciones de seguridad de correo electrónico para detectar e interceptar archivos adjuntos PDF que contengan JavaScript ofuscado o llamadas externas automatizadas hacia portales de descarga no categorizados.
4. Campañas enfocadas de concientización contra técnicas de Ingeniería Social: Capacitar al personal corporativo para identificar las tácticas recurrentes de esta amenaza, instruyendo sobre el riesgo de interactuar con documentos que aleguen estar "dañados" o "corruptos" y que demanden presionar botones de actualización o ejecutar comandos manuales en el sistema operativo (tácticas estilo ClickFix).

Prioridad: Urgente.

Ampliar información:

- https://osintsights.com/ousaban-trojan-targets-iberian-bank-users-with-sophisticated-pdf-lures
- https://thenextweb.com/news/ousaban-banking-trojan-spain-portugal-fake-pdf
- https://www.scworld.com/brief/ousaban-banking-trojan-targets-spain-and-portugal-with-new-stealth-techniques
- https://www.infosecurity-magazine.com/news/ousaban-banking-trojan-spain/
- https://thehackernews.com/2026/07/ousaban-banking-trojan-targets-iberian.html
- https://www.fortinet.com/blog/threat-research/analysis-of-ongoing-ousaban-attacks-targeting-the-iberian-peninsula

Recomendaciones generales sobre malware:

1. Actualizar el software y sistemas operativos regularmente, ya que los atacantes suelen explotar vulnerabilidades en software desactualizado.
2. Usar antivirus y herramientas antimalware confiables, manteniéndolos siempre al día.
3. Habilitar la autenticación multifactor (MFA) para proteger cuentas sensibles.
4. Evitar correos electrónicos y enlaces sospechosos, ya que el phishing es una de las principales vías de propagación de malware.
5. Realizar copias de seguridad regulares de archivos importantes para protegerse contra pérdidas en caso de ataques como el ransomware.
6. Limitar los privilegios de usuario, evitando el uso innecesario de cuentas con permisos de administrador.

NOTICIAS DE CIBERSEGURIDAD

EXPLOTACIÓN ACTIVA DE FALLO CRÍTICO EN ORACLE E-BUSINESS SUITE (CVE-2026-46817)

Se ha confirmado la explotación activa en entornos reales de una vulnerabilidad crítica de omisión de autenticación y gestión incorrecta de privilegios que afecta al módulo de procesamiento financiero Oracle Payments dentro de la plataforma de planificación de recursos empresariales (ERP) Oracle E-Business Suite (EBS). Detectada inicialmente a través de redes de honeypots a finales de junio de 2026, esta falla permite a atacantes remotos no autenticados comprometer el componente de transmisión de archivos y, potencialmente, tomar el control absoluto del módulo transaccional sin requerir credenciales válidas ni interacción del usuario.

Resumen técnico:

- Identificador principal: CVE-2026-46817.
- Severidad: Crítica (Puntaje base de 9.8 en la escala CVSS v3.1 / v4.0).
- Causa raíz: Fallas de validación de entrada e insuficiencia en los esquemas de control de acceso perimetral dentro del componente de transmisión de archivos (File Transmissions) de Oracle Payments. El fallo se categoriza bajo las debilidades CWE-306 (Falta de autenticación para una función crítica) y CWE-287 (Autenticación inapropiada).
- Mecanismo de falla: Los vectores de ataque dirigidos aprovechan el protocolo HTTP enviando solicitudes HTTP POST malformadas hacia el endpoint expuesto /OA_HTML/ibytransmit. Los atacantes inyectan una carga útil estructurada en XML diseñada para abusar del esquema de transmisión interno conocido como CODEX_PULL. Al procesar este XML malformado, la aplicación falla al validar los límites de ruta, habilitando una condición de Salto de Directorio (Path Traversal) o Inclusión de Archivos Locales (LFI) dentro de la Máquina Virtual de Java (JVM) del servidor de aplicaciones, lo que permite la lectura arbitraria de archivos del sistema operativo host (como /etc/passwd).
- Estado de explotación: Explotación activa confirmada en la naturaleza a partir del 27 de junio de 2026 por firmas de inteligencia de amenazas (Defused Cyber). Al tratarse de una vulnerabilidad de explotación automatizada y dirigida que actualmente no cuenta con código de prueba de concepto (PoC) público, se determina que los actores de amenazas están operando herramientas de explotación privadas (private weaponry) mediante escaneos de reconocimiento selectivos.
- Versiones afectadas: Oracle E-Business Suite versiones de la 12.2.3 a la 12.2.15 de forma inclusiva (específicamente el componente Oracle Payments).

Impacto potencial:

- Compromiso total del módulo de pagos (Takeover): La explotación exitosa concede al atacante control total sobre las funciones operativas de Oracle Payments, lo que compromete de manera directa la confidencialidad, integridad y disponibilidad de todo el sistema transaccional financiero de la organización.
- Exfiltración masiva de secretos y llaves de cifrado: Al abusar de la vulnerabilidad de inyección y lectura de archivos locales (LFI), los actores de amenazas pueden extraer archivos confidenciales de configuración del backend del ERP, lo que incluye cadenas de conexión con credenciales de bases de datos, llaves criptográficas institucionales o tokens de API vinculados a procesadores de pago externos.
- Facilitación de escalada de privilegios y persistencia interna: La recolección de archivos del sistema operativo expone la estructura de usuarios locales del servidor web. Esto permite a los atacantes mapear vectores de ataque complementarios para escalar privilegios hacia la cuenta del sistema o plantar persistencia silenciosa que se ejecute a nivel de la JVM del servidor de aplicaciones sin necesidad de generar balizas de red (beacons) salientes sospechosas.
- Alto riesgo de extorsión y despliegue de Ransomware: Históricamente, las fallas críticas de omisión de autenticación en soluciones ERP de Oracle han sido objetivos prioritarios para grupos de cibercrimen organizado y operadores de ransomware (como Cl0p y ShinyHunters) debido al alto valor de los datos almacenados (nóminas, datos bancarios de clientes, números de seguridad social), utilizándose como palanca para campañas masivas de robo de datos y doble extorsión.

Recomendaciones para mitigar el riesgo:

1. Aplicación inmediata de la actualización de seguridad oficial: Se urge a los administradores de sistemas ERP y CloudOps a desplegar con carácter de emergencia el parche correspondiente a la Actualización de Parches Críticos de Oracle (Critical Patch Update - CPU / CSPU) correspondiente a mayo de 2026.
2. Aislamiento y remoción de la exposición directa a Internet: Restrinja el acceso público a las interfaces web y endpoints de Oracle E-Business Suite. El acceso a la plataforma debe confinarse estrictamente detrás de redes privadas virtuales corporativas (VPN) o implementarse mediante arquitecturas de acceso a la red de confianza cero (ZTNA) para mitigar los escaneos perimetrales automatizados.
3. Aseguramiento mediante reglas específicas en el Web Application Firewall (WAF): Desplegar de forma inmediata firmas personalizadas en las soluciones WAF y sistemas de detección de intrusos (IDS) para inspeccionar, alertar y bloquear de manera proactiva cualquier solicitud HTTP POST dirigida a la URI /OA_HTML/ibytransmit, prestando especial atención a cargas XML que contengan la cadena de control CODEX_PULL o secuencias de escape de directorios (../).
4. Activación de procesos de Threat Hunting y Auditoría Forense: En caso de identificar instancias expuestas a internet que no hayan sido parchadas con anterioridad al 28 de mayo de 2026, se debe aplicar una postura de "asumir compromiso". Ejecute auditorías en los sistemas de logs web en busca de peticiones sospechosas al endpoint afectado y monitoree la creación de procesos secundarios inusuales originados desde el servicio Java de EBS. Si existen indicios de intrusión, inicie la rotación inmediata de todos los secretos, llaves y credenciales almacenadas en ese host.

Prioridad: Urgente.

Ampliar Información:

- https://socradar.io/blog/cve-2026-46817-oracle-payments-takeover/
- https://www.helpnetsecurity.com/2026/06/30/oracle-payments-cve-2026-46817-exploitation/
- https://devel.group/blog/explotacion-activa-de-vulnerabilidad-critica-en-oracle-e-business-suite-cve-2026-46817/
- https://thehackernews.com/2026/06/oracle-e-business-suite-flaw-cve-2026.html
- https://blog.elhacker.net/2026/06/vulnerabilidad-de-oracle-e-business.html
- https://www.ingenieriatelematica.com.co/vulnerabilidad-critica-cve-2026-46817-en-oracle-e-business-suite-bajo/
- https://laiadesk.com/blog/va/los-hackers-ya-explotan-una-grave-vulnerabilidad-de-oracle-e-business-en-sus-ata