GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º1526

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	3	0	0
MALWARE	0	1	0
NOTICIAS DE CIBERSEGURIDAD	0	0	1

VULNERABILIDADES

MÚLTIPLES VULNERABILIDADES EN PRODUCTOS FORTINET - CVE-2026-39808, CVE-2026-39813 y CVE-2026-22828

Fortinet ha publicado un conjunto de vulnerabilidades críticas que afectan a soluciones clave como FortiSandbox, FortiAnalyzer y FortiManager. Estos fallos permiten a atacantes remotos no autenticados ejecutar comandos en el sistema operativo, evadir mecanismos de autenticación mediante el uso de solicitudes HTTP manipuladas y comprometer la integridad de la infraestructura de gestión de seguridad.

Resumen técnico:

- Identificadores: CVE-2026-39808, CVE-2026-39813 y CVE-2026-22828.
- Severidad: Crítica (9.1) para los fallos en FortiSandbox y Alta (7.3) para FortiAnalyzer/Manager Cloud.
- Causa raíz: Fallos de inyección de comandos en la API (CWE-78), Path Traversal en la API JRPC (CWE-24) y desbordamiento de búfer basado en heap en el daemon oftpd (CWE-122).
- Mecanismo de falla: Un atacante puede enviar solicitudes HTTP especialmente manipuladas para evadir la autenticación, escalar privilegios o ejecutar código arbitrario directamente en el sistema operativo.
- Versiones afectadas: FortiSandbox 5.0.0 a 5.0.5 y 4.4.0 a 4.4.8; FortiAnalyzer y FortiManager Cloud versiones 7.6.2 a 7.6.4.

Impacto potencial:

- Ejecución remota de comandos: Permite que un atacante no autenticado ejecute código o comandos arbitrarios con privilegios del servicio afectado.
- Bypass de autenticación y toma de control: La explotación de vulnerabilidades de Path Traversal permite saltarse los controles de identidad y obtener acceso administrativo total.
- Compromiso de la infraestructura de gestión: El acceso no autorizado a herramientas centralizadas permite la manipulación de políticas de seguridad en toda la red corporativa.
- Persistencia y movimiento lateral: Facilita la creación de cuentas administrativas persistentes en el firmware y el pivoteo hacia otras redes de administración.

Recomendaciones de mitigación:

1. Actualización inmediata de firmware: Migrar urgentemente a las versiones corregidas: FortiSandbox 5.0.6 / 4.4.9 y FortiAnalyzer/Manager Cloud 7.6.5 o superiores.
2. Aplicación del principio de mínimo privilegio: Asegurar que los servicios se ejecuten con cuentas sin privilegios administrativos para limitar el impacto en caso de compromiso.
3. Aislamiento de la red de gestión: Restringir el acceso a todas las interfaces de gestión a una VLAN dedicada y aislada, bloqueando el enrutamiento desde redes no confiables.
4. Implementación de Jump Hosts y MFA: Obligar a que todo acceso administrativo pase por servidores de salto endurecidos que requieran autenticación multifactor obligatoria.

Prioridad: Crítica.

Ampliar información:

- https://csirt.telconet.net/comunicacion/noticias-seguridad/multiples-vulnerabilidades-criticas-en-productos-fortinet-permiten-ejecucion-remota-de-codigo-evasion-de-autenticacion-y-compromiso-de-sistemas/
- https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-fortinet-products-could-allow-for-arbitrary-code-execution_2026-035
- https://www.fortiguard.com/psirt/FG-IR-26-121
- https://www.fortiguard.com/psirt/FG-IR-26-112
- https://www.fortiguard.com/psirt/FG-IR-26-100

CVE-2026-33032 – BYPASS DE AUTENTICACIÓN EN NGINX-UI (MCPWN)

Se ha detectado una vulnerabilidad crítica, denominada "MCPwn", en la herramienta de gestión web nginx-ui que permite a atacantes no autenticados tomar el control total del servidor Nginx. El fallo reside en la implementación insegura del protocolo Model Context Protocol (MCP), específicamente en el endpoint /mcp_message, el cual carece de controles de autenticación y posee una lista blanca de IPs permitidas vacía por defecto, lo que el sistema interpreta como "permitir todo".

Resumen técnico:

- Identificador: CVE-2026-33032.
- Severidad: Crítica (9.8 según escala CVSS v3.1).
- Causa raíz: Falta de middleware de autenticación (AuthRequired()) en el endpoint /mcp_message y configuración predeterminada de IP permitidas insegura.
- Mecanismo de falla: Un atacante puede establecer una sesión mediante el endpoint /mcp y posteriormente enviar solicitudes POST al endpoint /mcp_message para invocar herramientas administrativas sin credenciales ni tokens.
- Versiones afectadas: Todas las versiones anteriores a la 2.3.4.}

Impacto potencial:

- Toma de control total del servicio: Capacidad para crear, modificar o eliminar archivos de configuración de Nginx y forzar recargas automáticas del servicio.
- Intercepción de tráfico sensible: Los atacantes pueden reconfigurar el servidor como un proxy inverso malicioso para capturar credenciales de administrador y datos en tránsito.
- Reconocimiento de infraestructura: Acceso a archivos de configuración que exponen la topología de la red interna, certificados TLS y direcciones de servicios críticos.
- Denegación de Servicio (DoS): Posibilidad de inyectar configuraciones inválidas que provoquen la caída del servidor y de todas las aplicaciones que dependen de él.

Recomendaciones de mitigación:

1. Actualización urgente: Migrar de forma inmediata a nginx-ui versión 2.3.4 o superior, la cual implementa los checks de autenticación necesarios.
2. Restricción de Red (Workaround): Modificar manualmente la lista blanca de IPs (IP whitelisting) pasando del estado predeterminado "allow-all" a "deny-all" o restringiéndola a hosts de confianza.
3. Desactivación de MCP: Como medida provisional, deshabilitar completamente la funcionalidad MCP si no es estrictamente necesaria para la operación del servidor.
4. Auditoría de Logs: Revisar exhaustivamente los registros de acceso en busca de solicitudes inusuales a los endpoints /mcp y /mcp_message que puedan indicar intentos de explotación previa.

Prioridad: Crítica.

Ampliar información:

- https://thehackernews.com/2026/04/critical-nginx-ui-vulnerability-cve.html
- https://securityaffairs.com/190841/hacking/cve-2026-33032-severe-nginx-ui-bug-grants-unauthenticated-server-access.html
- https://www.csoonline.com/article/4159248/critical-nginx-ui-tool-vulnerability-opens-web-servers-to-full-compromise.html
- https://www.darkreading.com/application-security/critical-mcp-integration-flaw-nginx-risk

CVE-2026-40261 & CVE-2026-40176 – RCE EN PHP COMPOSER VÍA MANIPULACIÓN DE PERFORCE VCS

Se han descubierto dos vulnerabilidades de alta severidad en Composer, el gestor de dependencias estándar para PHP, que permiten la ejecución remota de código (RCE) mediante la manipulación de repositorios Perforce. Un atacante puede explotar estos fallos al inducir a un usuario o sistema de integración continua (CI/CD) a procesar un archivo composer.json malicioso o metadatos de paquetes manipulados, permitiendo la inyección de comandos en el sistema operativo incluso si el software Perforce no está instalado.

Resumen técnico:

- Identificadores: CVE-2026-40261 (CVSS 8.8) y CVE-2026-40176 (CVSS 7.8).
- Severidad: Alta.
- Causa raíz: Validación insuficiente de entrada y falta de escape de caracteres especiales en los métodos syncCodeBase() y generateP4Command() del controlador VCS de Perforce.
- Mecanismo de falla: El atacante utiliza metacaracteres de shell en campos controlados por el usuario (como el puerto, usuario o referencias de origen); al construir el comando de sistema, Composer ejecuta las instrucciones inyectadas con los privilegios del usuario actual.
- Versiones afectadas: Versiones 2.x anteriores a la 2.9.6 y versiones 1.x anteriores a la 2.2.27 (LTS).

Impacto potencial:

- Ejecución de comandos arbitrarios: Compromiso total de la estación de trabajo del desarrollador o del servidor de compilación afectado.
- Vulneración de la cadena de suministro: Posibilidad de inyectar código malicioso en aplicaciones legítimas durante el proceso de empaquetado y despliegue automático.
- Robo de propiedad intelectual: Acceso no autorizado al código fuente local y a las credenciales de otros servicios integrados en el entorno de desarrollo.
- Pérdida de integridad en entornos CI/CD: Manipulación de los artefactos de salida en servidores de integración, afectando a múltiples usuarios finales de la aplicación.

Recomendaciones de mitigación:

1. Actualización inmediata: Ejecutar el comando composer self-update para instalar las versiones corregidas (2.9.6 o 2.2.27).
2. Preferencia por instalaciones 'dist': Configurar el uso de --prefer-dist o establecer preferred-install: dist en la configuración global para evitar la descarga desde fuentes VCS vulnerables.
3. Inspección de proyectos externos: Revisar minuciosamente los archivos composer.json de proyectos no confiables antes de ejecutar cualquier comando de Composer en ellos.
4. Limitación de repositorios: Utilizar exclusivamente repositorios de paquetes (Packagist) de confianza y deshabilitar el soporte de Perforce si no es estrictamente necesario para la organización.

Prioridad: Crítica.

Ampliar información:

- https://laravel-news.com/composer-296-fixes-two-perforce-command-injection-vulnerabilities
- https://community.opentextcybersecurity.com/vulnerability-vault-228/php-composer-flaws-enable-remote-command-execution-via-perforce-vcs-364048
- https://securityaffairs.com/190824/security/php-composer-flaws-enable-remote-command-execution-via-perforce-vcs.html
- https://www.cryptika.com/new-php-composer-vulnerability-let-attackers-execute-arbitrary-commands/
- https://thehackernews.com/2026/04/new-php-composer-flaws-enable-arbitrary.html

MALWARE

MIRAX – ANDROID REMOTE ACCESS TROJAN (RAT) CON CAPACIDADES DE PROXY RESIDENCIAL

Se ha identificado una campaña masiva del nuevo troyano de acceso remoto (RAT) denominado Mirax, que ha afectado a más de 220,000 cuentas, principalmente en España y otros países de habla hispana. Este malware se distribuye a través de anuncios maliciosos en plataformas de Meta (Facebook, Instagram, Messenger) y aplicaciones falsas de IPTV. Su peligrosidad radica en que no solo roba credenciales bancarias y de criptoactivos, sino que convierte los dispositivos infectados en nodos de proxy SOCKS5, permitiendo a los atacantes enmascarar actividades criminales bajo la dirección IP legítima de la víctima.

Resumen técnico:

- Identificador: Mirax Android RAT (comercializado como Malware-as-a-Service).
- Severidad: Crítica / Urgente.
- Causa raíz: Abuso de los Servicios de Accesibilidad de Android y tácticas de ingeniería social mediante publicidad maliciosa (malvertising).
- Mecanismo de falla: El malware utiliza un dropper (alojado en GitHub) que solicita permisos de accesibilidad. Una vez concedidos, despliega capas de superposición (overlays) dinámicas sobre 182 aplicaciones (banca, cripto y redes sociales) para capturar credenciales y utiliza protocolos como SOCKS5 y Yamux para crear túneles de comunicación con el C2.
- Plataformas afectadas: Dispositivos móviles con sistema operativo Android.

Impacto potencial:

- Control total remoto y VNC: Los atacantes pueden visualizar la pantalla en tiempo real, ejecutar comandos y navegar por la interfaz del usuario para realizar transferencias no autorizadas.
- Conversión en proxy residencial: El dispositivo se integra en una botnet que vende el tráfico de red de la víctima para evadir sistemas de detección de fraude y bloqueos geográficos en otros ataques.
- Exfiltración de datos biométricos y de bloqueo: Capacidad para capturar el PIN, patrones de desbloqueo, estructura de seguridad del dispositivo y uso de biometría.
- Vigilancia y espionaje continuo: Incluye módulos de keylogging persistente, captura de fotos con la cámara y lectura de todos los mensajes SMS para interceptar códigos de verificación (OTP).

Recomendaciones de mitigación:

1. Restricción de fuentes desconocidas: Deshabilitar la opción de "Instalar aplicaciones de fuentes desconocidas" y evitar la descarga de APKs fuera de Google Play Store, especialmente de servicios de IPTV.
2. Auditoría de Servicios de Accesibilidad: Revisar periódicamente en los ajustes del sistema qué aplicaciones poseen permisos de accesibilidad y revocar el acceso a cualquier herramienta no esencial o sospechosa.
3. Protección de red y DNS: Implementar soluciones de filtrado de contenido que bloqueen el acceso a dominios de distribución conocidos (como descarga-smtr[.]net) y servidores de comando y control (ilovepng[.]info).
4. Implementación de soluciones MTD: Utilizar herramientas de Mobile Threat Defense (MTD) capaces de detectar comportamientos anómalos, como la creación de túneles SOCKS5 o el uso de inyecciones de HTML dinámicas.

Prioridad: Urgente.

Ampliar información:

- https://www.antifraude.co/mirax-android-rat-convierte-dispositivos-en-bots-para-ataques-masivos-y-robo-de-datos/
- https://www.securityweek.com/mirax-rat-targeting-android-users-in-europe/
- https://thehackernews.com/2026/04/mirax-android-rat-turns-devices-into.html
- https://securityaffairs.com/190842/uncategorized/mirax-malware-campaign-hits-220k-accounts-enables-full-remote-control.html
- https://www.cleafy.com/cleafy-labs/mirax-a-new-android-rat-turning-infected-devices-into-potential-residential-proxy-nodes

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

ABUSO DE WEBHOOKS EN n8n PARA CAMPAÑAS DE PHISHING Y MALWARE

Se ha identificado un uso sostenido de la plataforma de automatización de flujos de trabajo n8n por parte de actores de amenazas para orquestar campañas de phishing sofisticadas. Los atacantes aprovechan la infraestructura legítima de la plataforma, específicamente los subdominios bajo *.app.n8n.cloud, para evadir filtros de seguridad tradicionales y entregar cargas útiles maliciosas o realizar el "fingerprinting" de dispositivos. Este método permite que los correos y enlaces maliciosos hereden la reputación de dominio y los certificados TLS confiables del proveedor.

Resumen técnico:

- Identificador: Abuso de infraestructura SaaS (n8n Webhooks).
- Severidad: Importante (Facilita la persistencia y evasión).
- Causa raíz: Exposición de webhooks URL sin autenticación obligatoria en cuentas de desarrollador o de prueba de n8n.
- Mecanismo de falla: Los atacantes crean flujos de trabajo que actúan como "listeners" de solicitudes HTTP. Al ser accedidos, estos webhooks sirven dinámicamente páginas de phishing con CAPTCHA o píxeles de seguimiento invisibles, descargando malware (como instaladores MSI o ejecutables) directamente desde el dominio de n8n a través de scripts encapsulados.
- Plataformas afectadas: Infraestructura de red y seguridad de correo que confía en listas blancas de servicios SaaS.

Impacto potencial:

- Evasión de filtros de reputación: Los enlaces de n8n no suelen estar bloqueados, lo que permite que el contenido malicioso llegue a la bandeja de entrada del usuario final.
- Entrega de herramientas de acceso remoto (RMM): Se ha observado la distribución de versiones modificadas de herramientas legítimas como Datto e ITarian para establecer persistencia en la red corporativa.
- Fingerprinting y reconocimiento: El uso de píxeles de seguimiento permite a los atacantes identificar qué usuarios abren los correos, recolectando datos como direcciones IP y versiones de navegadores para futuros ataques dirigidos.
- Automatización de ataques a escala: El uso de IA y flujos de trabajo automáticos incrementa drásticamente el volumen de correos enviados, registrando aumentos de hasta el 686% en la actividad de estos webhooks.

Recomendaciones para mitigar el riesgo:

1. Monitoreo de telemetría de red: Implementar reglas de detección que alerten sobre comunicaciones salientes hacia subdominios de *.app.n8n.cloud que no correspondan a flujos de trabajo autorizados por la organización.
2. Revisión de listas blancas (Allowlists): Evitar la confianza ciega en dominios de proveedores SaaS y aplicar inspección de contenido (SSL/TLS Inspection) incluso en tráfico hacia nubes conocidas.
3. Seguridad de correo con IA: Utilizar soluciones de seguridad de correo electrónico que empleen procesamiento de lenguaje natural (NLP) para detectar la intención maliciosa detrás de enlaces aparentemente legítimos.
4. Bloqueo preventivo de indicadores: Considerar el bloqueo o escrutinio de subdominios específicos identificados en investigaciones de inteligencia (ej. tti.app.n8n.cloud) dentro de los sistemas de filtrado web y gateways de correo.

Prioridad: Importante.

Ampliar Información:

- https://blog.talosintelligence.com/the-n8n-n8mare/
- https://thehackernews.com/2026/04/n8n-webhooks-abused-since-october-2025.html
- https://letsdatascience.com/news/n8n-webhooks-deliver-malware-in-phishing-campaigns-616f8be8