GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º3326

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 para nuestros 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	1	0

VULNERABILIDADES

GITLAB – INYECCIÓN DE CÓDIGO Y MODIFICACIÓN/ELIMINACIÓN NO AUTENTICADA DE PROYECTOS VÍA GRAPHQL (CVE-2026-19478 / CVE-2026-19650)

GitLab ha publicado de manera urgente una actualización de seguridad fuera de su ciclo habitual para corregir una vulnerabilidad crítica (CVSS 9.4) en las ediciones Community (CE) y Enterprise (EE) autogestionadas (self-managed). El fallo, radicado en la API de GraphQL, permite a atacantes remotos no autenticados modificar o eliminar proyectos públicos y datos de usuarios sin requerir credenciales ni interacción de la víctima.

Resumen técnico:

- Identificador principal: CVE-2026-19478 (Acompañado de CVE-2026-19650).
- Severidad: Crítica (CVSS v3.1: 9.4 / Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H).
- Causa raíz: Inyección de código mediante procesamiento y validación incorrecta de directivas en GraphQL (CWE-94 / CWE-862).
- Mecanismo de falla: El motor de GraphQL procesa determinadas directivas internas antes de ejecutar las comprobaciones de autorización a nivel de campo. Al no asignar un resolutor explícito, el sistema recurre al comportamiento por defecto, ejecutando métodos del objeto subyacente basados en nombres controlados por la petición. Esto permite omitir los controles de acceso e invocar operaciones destructivas de modificación o borrado de datos sin requerir token ni sesión activa.
- Estado de explotación: Divulgada oficialmente por GitLab el 17 de agosto de 2026 mediante un parche de emergencia fuera de ciclo. No se registra evidencia de explotación activa en el entorno real ni prueba de concepto (PoC) pública al momento de la publicación. Las plataformas SaaS (GitLab.com y Dedicated) fueron parcheadas automáticamente por el fabricante.
- Versiones afectadas: GitLab CE/EE ramas 18.2 hasta versiones anteriores a 18.11.11; 19.0 anteriores a 19.0.8; 19.1 anteriores a 19.1.6; y 19.2 anteriores a 19.2.4.

Impacto potencial:

- Destrucción y alteración no autorizada de proyectos públicos: Un atacante anónimo que alcance el endpoint de la API puede borrar o modificar repositorios, historiales de código, artefactos e issues pertenecientes a proyectos con visibilidad pública.
- Evasión total de controles de autenticación y autorización: La falla en la secuencia de evaluación de directivas de GraphQL permite que peticiones remotas ejecuten instrucciones sobre el sistema ignorando la validación de credenciales, roles o permisos de usuario.
- Sabotaje a la cadena de suministro de software y datos de usuario: La eliminación masiva o alteración maliciosa de activos públicos impacta gravemente la disponibilidad de los desarrollos corporativos y la integridad de la infraestructura de integración continua (CI/CD).
- Riesgo secundario por mutaciones no autorizadas vía GET (CSRF / CVE-2026-19650): El boletín resuelve además un fallo de severidad alta (CVSS 7.1) que permite a atacantes inducir la ejecución de mutaciones en el manejador de consultas multiplexadas mediante solicitudes HTTP GET engañosas.

Recomendaciones de mitigación:

1. Actualización prioritaria de instancias self-managed: Aplicar de inmediato los parches de seguridad oficiales lanzados para las respectivas ramas de versión: 19.2.4, 19.1.6, 19.0.8 o 18.11.11.
2. Restricción perimetral del endpoint GraphQL (Mitigación temporal): De no ser posible la actualización inmediata, implementar reglas de filtrado en el WAF o proxy inverso (p. ej., Nginx) para limitar el acceso a /api/graphql únicamente a subredes o direcciones IP de confianza.
3. Auditoría de registros API y monitoreo de integridad: Revisar los logs de acceso al endpoint de GraphQL en busca de peticiones anómalas que contengan directivas poco habituales o bursts de solicitudes anónimas, y contrastar el estado de los repositorios públicos con respaldos recientes.
4. Aislamiento de red y gestión de visibilidad de proyectos: Restringir temporalmente la visibilidad de los proyectos de "Público" a "Privado" o "Interno" y aislar la instancia de redes no seguras mientras se planifica la ventana de actualización.

Prioridad: Crítica.

Ampliar información:

- https://cloud.donweb.com/gitlab-cve-2026-19478-un-graphql-que-borra-proyectos-sin-login/
- https://thehackernews.com/2026/08/critical-gitlab-graphql-flaw-could-let.html
- https://socprime.com/blog/cve-2026-19478-analysis/
- https://devel.group/blog/vulnerabilidad-critica-en-gitlab-graphql-permite-borrado-remoto-de-proyectos-publicos/
- https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-2-4-released/
- https://csirt.telconet.net/comunicacion/boletines-servicios/vulnerabilidad-critica-en-gitlab-graphql-permite-a-atacantes-eliminar-proyectos-publicos-sin-autenticacion/

FORMINATOR FORMS – CARGA ARBITRARIA DE ARCHIVOS Y EJECUCIÓN REMOTA DE CÓDIGO SIN AUTENTICACIÓN (CVE-2026-15748)

Se ha divulgado una vulnerabilidad crítica (CVSS 9.8) que afecta al popular plugin de formularios para WordPress Forminator Forms, instalado en más de 600.000 sitios web activos. El fallo permite a atacantes remotos no autenticados subir archivos PHP maliciosos y lograr la ejecución remota de código (RCE), lo que faculta el control total sobre los servidores y sitios web comprometidos.

Resumen técnico:

- Identificador principal: CVE-2026-15748.
- Severidad: Crítica (CVSS v3.1: 9.8/ VectorCVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).
- Causa raíz: Carga de archivos no restringida con tipo peligroso (CWE-434) e insuficiente validación de tipos de archivo en la función handle_file_upload().
- Mecanismo de falla: Un atacante puede explotar un formulario publicado que contenga simultáneamente un campo de selección (Select) y un campo de subida de archivos (File Upload). Al inyectar configuraciones manipuladas a través del campo Select, el plugin las procesa como legítimas. Posteriormente, evade la lista negra de extensiones peligrosas utilizando patrones de nombres de archivos y mapas MIME alternativos (como ph(p)|text/x-php) que eluden la coincidencia exacta del filtro pero son interpretados por WordPress como PHP. Si los archivos se almacenan en directorios personalizados sin protección .htaccess activa, solicitar el archivo ejecuta el código en el servidor.
- Estado de explotación: Descubierta e informada en julio de 2026, detallada públicamente a mediados de agosto de 2026. Aunque no se registraba explotación masiva en el momento de la divulgación pública, dada la disponibilidad del parche y la simplicidad de la prueba de concepto, representa una superficie de ataque prioritaria para escáneres automatizados.
- Versiones afectadas: Forminator Forms versiones 1.56.1 y todas las anteriores. Corregido en la versión 1.56.2 (disponible desde el 31 de julio de 2026).

Impacto potencial:

- Ejecución remota de código (RCE) y control total del sitio: Un atacante anónimo puede subir webshells e instrucciones ejecutables, tomando el control administrativo del entorno WordPress y del servidor web anfitrión.
- Exfiltración de bases de datos y credenciales sensibles: Permite leer archivos de configuración críticos como wp-config.php, exponiendo usuarios, claves secretas y credenciales de la base de datos MySQL.
- Creación de cuentas administrativas no autorizadas y persistencia: Facilita la inyección de código malicioso, alteración de archivos core o la creación discreta de nuevos usuarios con rol de administrador para mantener acceso a largo plazo.
- Propagación de malware y movimiento lateral: Otorga la capacidad de redirigir a los visitantes hacia sitios de phishing/spam e infectar otros sitios web alojados en el mismo servidor en entornos de hosting compartido.

Recomendaciones de mitigación:

1. Actualización inmediata del plugin: Actualizar Forminator Forms de manera prioritaria a la versión 1.56.2 o superior en todas las instancias de WordPress de producción y desarrollo.
2. Inspección y auditoría de directorios de subida: Auditar de forma exhaustiva la carpeta /wp-content/uploads/ y rutas personalizadas en busca de archivos .php, .phtml o extensiones anómalas (p. ej., ph(p)).
3. Endurecimiento del servidor web (Server Hardening): Configurar reglas globales en el servidor web (Apache o Nginx) que impidan estrictamente la ejecución de scripts PHP en todos los directorios destinados al almacenamiento de archivos adjuntos.
4. Auditoría de seguridad y revisión de formularios públicos: Verificar qué formularios públicos combinan campos Select y File Upload, e inspeccionar logs del servidor y cuentas de usuarios recientes para descartar indicadores de compromiso (IoC) previos al parche.

Prioridad: Crítica.

Ampliar información:

- https://thehackernews.com/2026/08/forminator-wordpress-flaw-can-enable.html
- https://www.wordfence.com/blog/2026/08/600000-wordpress-sites-affected-by-arbitrary-file-upload-vulnerability-in-forminator-forms-wordpress-plugin/
- https://socprime.com/blog/cve-2026-15748-analysis/
- https://seguridadenwordpress.com/vulnerabilidad-forminator-wordpress-cve-2026-15748/
- https://devel.group/blog/vulnerabilidad-critica-cvss-9-8-en-wordpress-forminator-permite-rce/

MICROSOFT COPILOT PERSONAL – CADENA DE VULNERABILIDADES "COSNITCH" PERMITE EJECUCIÓN AUTOMÁTICA DE PROMPTS Y EXFILTRACIÓN SILENCIOSA DE DATOS (CVE-2026-24301)

Varonis Threat Labs ha divulgado un conjunto de tres vulnerabilidades encadenadas en la versión personal de Microsoft Copilot (copilot.microsoft.com), denominadas colectivamente CoSnitch (CVE-2026-24301). La falla permite a un atacante, mediante un solo clic de la víctima en un enlace malicioso, ejecutar instrucciones de forma automática para consultar aplicaciones conectadas (como Gmail, Google Drive y Calendar) y exfiltrar datos sensibles hacia servidores externos sin generar alertas visibles.

Resumen técnico:

- Identificador principal: CVE-2026-24301 (Denominación clave: CoSnitch).
- Severidad: Crítica (Afecta la confidencialidad e integridad del entorno del asistente).
- Causa raíz: Falta de controles de interacción del usuario en parámetros de URL, abuso de capacidades legítimas de extracción web (web fetching) y susceptibilidad a inyección indirecta de instrucciones (Indirect Prompt Injection) en la memoria persistente del modelo.
- Mecanismo de falla: Se basa en tres fallas encadenadas: 1) Ejecución automática de prompts al cargar la página combinando el parámetro ?q= con el parámetro no documentado autorun=1; 2) Exfiltración silenciosa de datos utilizando conectores OAuth autorizados (Gmail, Google Drive, Calendario, etc.), codificando los resultados en Base64 e instruyendo a Copilot a realizar una petición HTTP GET a un webhook del atacante; 3) Envenenamiento de memoria persistente vía resumen de páginas web maliciosas, lo que inyecta instrucciones permanentes que persisten tras cambios de contraseña o cierres de sesión.
- Estado de explotación: Divulgada a Microsoft en diciembre de 2025 y corregida oficialmente el 18 de agosto de 2026 mediante parches del lado del servidor. No se registra evidencia de explotación activa en el entorno real al momento de la publicación. La vulnerabilidad fue descubierta mediante la técnica de meta-hacking (ingeniería social aplicada al motor de razonamiento del LLM).
- Versiones afectadas: Plataforma web de Microsoft Copilot Personal (copilot.microsoft.com).

Impacto potencial:

- Exfiltración silenciosa de datos sensibles e información corporativa: Un atacante puede extraer el contenido completo de correos electrónicos, credenciales en texto plano, eventos de calendario, archivos almacenados en la nube e historial de chats con un simple clic.
- Ejecución remota e inmediata de prompts sin interacción (One-Click): La combinación de parámetros de URL permite disparar instrucciones completas del LLM en la sesión autenticada de la víctima de manera automática e inadvertida.
- Compromiso y envenenamiento persistente de la memoria del LLM: La inyección indirecta modifica la memoria a largo plazo del asistente, haciendo que persistan instrucciones maliciosas o desinformación en sesiones futuras sin que el usuario lo note.
- Evasión de controles de seguridad de red: La exfiltración se realiza mediante solicitudes HTTP GET legítimas iniciadas por la infraestructura propia de Microsoft, lo que impide que las herramientas tradicionales de seguridad detecten patrones anómalos o sospechosos.

Recomendaciones de mitigación:

1. Auditoría y reducción de conectores OAuth activos: Revisar minuciosamente las aplicaciones integradas al asistente (Gmail, Google Drive, OneDrive) y desvincular los servicios que no sean estrictamente requeridos.
2. Inspección de enlaces y parámetros URL hacia asistentes de IA: Instruir a los usuarios sobre los riesgos de abrir enlaces externos que apunten a plataformas de IA, especialmente aquellos que incorporen parámetros de consulta o ejecuciones preconfiguradas.
3. Revisión y limpieza manual de la memoria persistente: Inspeccionar periódicamente la configuración de memoria de Copilot para verificar la ausencia de reglas o instrucciones persistentes desconocidas depositadas por fuentes externas.
4. Principio de menor privilegio y monitoreo de telemetría: Tratar los asistentes de IA como usuarios con privilegios dentro de la red corporativa e implementar herramientas de monitoreo enfocadas en detectar patrones anómalos de lectura y consulta de datos masivos.

Prioridad: Crítica.

Ampliar información:

- https://infosecdash.com/noticia.html?n=vulnerabilidades-en-microsoft-copilot-permiten-robo-de-datos-con-un-solo-clic-pbh11qf
- https://www.computerworld.com/article/4211325/microsoft-finally-patches-critical-one-click-copilot-vulnerability-more-than-eight-months-after-learning-of-it.html
- https://cybersecuritynews.com/copilot-cosnitch-vulnerability/amp/
- https://thehackernews.com/2026/08/microsoft-copilot-personal-flaws-could.html
- https://www.varonis.com/blog/cosnitch

MALWARE

EVOOO1BOT – BOTNET MULTIFUNCIONAL PARA LINUX TRANSFORMA DISPOSITIVOS PERIMETRALES EN PROXIES SOCKS5 Y PLATAFORMAS DE ATAQUE

FortiGuard Labs ha descubierto una nueva familia de botnets para sistemas Linux denominada Evooo1Bot, la cual evoluciona el motor de código abierto de Mirai incorporando un marco modular de administración remota. La amenaza compromete dispositivos perimetrales expuestos a Internet (como routers, cortafuegos, cámaras IP y RTUs) para convertirlos en proxies de red persistentes, realizar escaneos de credenciales corporativas y ejecutar ataques de denegación de servicio (DDoS).

Resumen técnico:

- Identificador principal: Campaña Flooding / Botnet Evooo1Bot (Identificada por la cadena "evooo1" presente en sus binarios).
- Tipo de amenaza: Botnet para sistemas Linux, Troyano de Acceso Remoto (RAT), Enrutador Proxy SOCKS5, Escáner SSH y Motor DDoS.
- Mecanismo de acceso e infección: Explotación automatizada de múltiples vulnerabilidades conocidas (algunas históricas como CVE-2007-3010 y CVE-2016-6277, hasta recientes como CVE-2024-29269 y CVE-2025-10123) en equipos de fabricantes como Alcatel, NETGEAR, Tenda, D-Link, Mitsubishi y Telesquare. Tras la explotación, descarga y ejecuta el script cargador wget.sh desde el servidor 91.92.40[.]118.
- Capacidades avanzadas y evasión: Incorpora cifrado de cadenas multicapa (AES-256-CTR, ChaCha20 y XOR), evasión de entornos de análisis (sandboxes y honeypots como Cowrie o Kippo), y canal de comunicaciones C2 cifrado a través del puerto TCP 443 para camuflarse con el tráfico HTTPS legítimo.

- Módulos integrados: Módulo de proxy SOCKS5 (directo y reverso), sniffer de credenciales (captura encabezados de autorización HTTP y cookies desde /proc/net/tcp), escáner de fuerza bruta SSH con un diccionario de más de 150 credenciales enfocadas en entornos corporativos/IoT, y motor DDoS con 16 vectores de ataque.
- Mecanismos de persistencia: Instalación simultánea mediante un servicio systemd que suplanta a Apache HTTPD (Apache HTTPD Cache Manager), scripts init SysV, tareas en cron cada 5 minutos, inyección en /etc/profile.d/ y modificación de /etc/rc.local. Además, manipula /proc/self/oom_score_adj y bloquea /dev/watchdog para prevenir reinicios del sistema.
- Estado de actividad: Actividad masiva detectada en el entorno real desde julio de 2026, con reportes y análisis técnicos divulgados a mediados de agosto de 2026.

Impacto potencial:

- Conversión de equipos en infraestructura de ataque (Proxies SOCKS5): El módulo de proxy reverso permite enrutar tráfico TCP arbitrario a través de la dirección IP pública de la víctima, ocultando el origen real del atacante o comercializando la red comprometida como un servicio de proxy residencial o corporativo.
- Punto de apoyo para movimiento lateral e intrusión interna: El compromiso de firewalls, routers y dispositivos de borde proporciona a los atacantes una presencia persistente dentro del perímetro corporativo, permitiéndoles pivotar hacia sistemas y redes internas de la organización.
- Interceptación de datos sensibles y credenciales corporativas: El componente de captura (sniffer) analiza el tráfico local para interceptar cookies de sesión y encabezados de autenticación HTTP Basic en texto plano, almacenándolos en /tmp/.sniff.log para su posterior exfiltración.
- Generación de ataques de denegación de servicio masivos (DDoS): Reutiliza y amplía el motor de Mirai con 16 vectores de saturación (UDP, TCP SYN/ACK, DNS, HTTP flood y amplificación VSE), capaces de degradar o tumbar servicios críticos en la red.

Recomendaciones de mitigación:

1. Actualización y parcheo prioritario de dispositivos de borde: Aplicar parches y actualizar el firmware de routers, cortafuegos, cámaras IP y RTUs, retirando o aislando los equipos obsoletos (legacy) que ya no cuenten con soporte del fabricante.
2. Bloqueo de Indicadores de Compromiso (IoC) e infraestructura C2: Configurar reglas en firewalls y DNS corporativos para bloquear las conexiones salientes hacia la dirección IP de carga identificada (91.92.40[.]118) y supervisar conexiones inusuales por el puerto TCP 443 hacia destinos no confiables.
3. Auditoría de persistencia y procesos anómalos en hosts Linux: Inspeccionar la presencia de servicios systemd sospechosos, tareas no autorizadas en crontab, scripts en /etc/profile.d/ y archivos ocultos en la carpeta /tmp/.
4. Hardening de servicios SSH e implementación de segmentación de red: Deshabilitar la autenticación por contraseña en servidores y dispositivos expuestos a favor de llaves SSH, bloquear nombres de usuario por defecto y aislar las interfaces de administración de la red pública.

Prioridad: Urgente.

Ampliar información:

- https://csirtasobancaria.com/alertas-de-seguridad/evooo1bot-nueva-botnet-multifuncional-para-linux-con-capacidades-de-administracion-remota-y-operaciones-de-red
- https://www.fortinet.com/blog/threat-research/multi-functional-linux-botnet-evooo1bot
- https://socprime.com/active-threats/evooo1bot-linux-botnet-capabilities-and-attack-techniques/
- https://fastnetmon.com/2026/08/19/ddos-news-evooo1bot-linux-botnet-hijacks-routers-and-firewalls/
- https://thehackernews.com/2026/08/evooo1bot-linux-botnet-exploits-known.html
- https://www.darkreading.com/cyber-risk/linux-botnet-evooo1bot-mirai-capabilities-beyond-ddos

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

MLFLOW Y FUXA – EXPLOTACIÓN ACTIVA DE VULNERABILIDADES CRÍTICAS EN PLATAFORMAS DE IA Y AUTOMATIZACIÓN INDUSTRIAL (CVE-2026-64849 / CVE-2026-25895)

Se han detectado campañas masivas de escaneo y explotación activa dirigidas a dos populares plataformas de código abierto: MLflow (gestión del ciclo de vida de modelos de inteligencia artificial) y FUXA (sistema SCADA/HMI para automatización industrial). Las fallas permiten la exfiltración de credenciales en la nube y la ejecución remota de código, representando un riesgo crítico para entornos de ciencia de datos e infraestructura operacional (OT).

Resumen técnico:

- Identificador principal: CVE-2026-64849 (MLflow) / CVE-2026-25895 (FUXA).
- Severidad: Crítica (CVSS v3.1: 9.3 para MLflow / CVSS v3.1: 9.5 para FUXA).
- Causa raíz: Falsificación de solicitudes del lado del servidor (SSRF) en webhooks de MLflow (CWE-918); y omisión de autenticación junto a salto de directorio (path traversal) en FUXA (CWE-22 / CWE-306).
- Mecanismo de falla: En MLflow, el fallo en la validación de URLs en webhooks de model-registry combina redirecciones HTTP con DNS rebinding para evadir filtros y consultar los endpoints de metadatos de instancias cloud (AWS, Azure, GCP), extrayendo credenciales y secretos. En FUXA, la ausencia de autenticación por defecto y la navegación arbitraria por directorios permiten a un atacante no autenticado escribir o sobrescribir archivos del sistema (como main.js) para lograr la ejecución remota de código (RCE) en el servidor SCADA.
- Estado de explotación: Explotación activa confirmada en el entorno real iniciada pocas horas después de su divulgación el 17 y 18 de agosto de 2026 por firmas como watchTowr y VulnCheck. CISA añadió la vulnerabilidad de MLflow (CVE-2026-64849) a su catálogo KEV el 19 de agosto de 2026.
- Versiones afectadas: MLflow en versiones anteriores a 3.15.0; FUXA en versiones 1.2.9 y anteriores.

Impacto potencial:

- Exfiltración de credenciales y secretos en la nube (MLflow): La explotación del SSRF otorga acceso directo a las APIs de metadatos de la infraestructura cloud, exponiendo tokens temporales, llaves de acceso e información confidencial de la organización.
- Control total de plataformas SCADA/HMI e interrupción industrial (FUXA): La capacidad de escribir archivos en FUXA abre la puerta al despliegue de código malicioso en el sistema que opera líneas de producción, amenazando la continuidad operativa y la seguridad de procesos industriales.
- Exposición por falta de autenticación habilitada por defecto: Ambos sistemas suelen desplegarse sin credenciales activadas por omisión, lo que permite a bots y atacantes escanear la red e infectar de forma automática instancias expuestas a Internet.
- Pivote lateral hacia repositorios de IA e infraestructura interna: El compromiso de servidores de desarrollo de ML/IA expone pipelines de datos, modelos propietarios y componentes centrales de la red corporativa.

Recomendaciones para mitigar el riesgo:

1. Actualización prioritaria de software: Actualizar de inmediato las instancias de MLflow a la versión 3.15.0 o superior, y FUXA a versiones posteriores a la 1.2.9.
2. Habilitación de autenticación y controles de acceso estrictos: Garantizar la activación obligatoria de mecanismos de autenticación y autorización en todos los paneles e interfaces de MLflow y FUXA.
3. Restricción perimetral y segmentación de red: Aislar los entornos de automatización industrial (OT) y servidores MLOps detrás de firewalls/VPNs, impidiendo el acceso directo o exposición a la Internet pública.
4. Rotación de credenciales y endurecimiento de metadatos cloud: Rotar inmediatamente las claves o tokens asociados a las cargas de trabajo de MLflow expuestas y bloquear/limitar el acceso a los servicios de metadatos desde aplicaciones que no lo requieran.

Prioridad: Urgente.

Ampliar Información:

- https://thehackernews.com/2026/08/attackers-exploit-mlflow-ssrf-flaw-to.html
- https://servola.de/es/journal/two-open-source-tools-were-hacked-hours-after-disclosure/
- https://infosecdash.com/noticia.html?n=detectan-ataques-contra-vulnerabilidades-criticas-en-mlflow-y-fuxa-ywd4ok4
- https://cyberexperts.com/2026-08-19-attackers-exploit-mlflow-ssrf-flaw-to-steal-cloud-credentials-and-secrets/
- https://www.theexploitdesk.tech/article/attackers-exploit-mlflow-ssrf-flaw-to-steal-cloud-credentials-and-secr-de6e4c