GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °3426

TLP:GREEN
TRAFFIC LIGHT PROTOCOL
https://www.first.org/tlp/

BOLETÍN CIBERSEGURIDAD
SEMANAL EDICIÓN º3426

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

KALTURA MWEMBED – DESERIALIZACIÓN NO SEGURA EN PHP PERMITE LECTURA ARBITRARIA DE ARCHIVOS Y EJECUCIÓN REMOTA DE CÓDIGO SIN AUTENTICACIÓN (CVE-2026-19913 / CVE-2026-19912)

Se han divulgado dos vulnerabilidades críticas no parcheadas (CVE-2026-19913 y CVE-2026-19912) en la librería del reproductor de video HTML5 de Kaltura (mwEmbed / html5lib), utilizada ampliamente en aplicaciones web e infraestructura CDN multi-tenant. Los fallos radican en una deserialización de PHP no segura en el endpoint mwEmbedLoader.php, facultando a atacantes remotos no autenticados a leer archivos confidenciales del servidor y lograr la ejecución remota de código (RCE) sin requerir credenciales ni sesión previa.

Resumen técnico:

- Identificador principal: CVE-2026-19913 (Lectura de archivos) / CVE-2026-19912 (Ejecución remota de código - RCE).
- Severidad: Crítica (CVSS v3.1: 10.0 / 9.1 asignado por investigadores / Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).
- Causa raíz: Deserialización de datos no confiables en PHP (CWE-502), validación insuficiente del esquema de URL y salto de directorio (Path Traversal / CWE-22).
- Mecanismo de falla: El endpoint mwEmbedLoader.php procesa el parámetro ServiceUrl pasando la respuesta directamente a unserialize() sin validar el origen o protocolo. Al enviar un esquema file://, la aplicación intenta deserializar el archivo local; al fallar, incluye los datos crudos del archivo dentro del mensaje de error (CVE-2026-19913). Por otro lado, la falta de sanitización del parámetro uiconf_id permite inyectar secuencias ../ para redirigir la escritura de datos deserializados con código PHP malicioso fuera de la caché y depositar una webshell en un directorio accesible vía web, ejecutando comandos en el servidor (CVE-2026-19912).
- Estado de explotación: Divulgadas públicamente el 25 y 26 de agosto de 2026 por el CERT/CC tras intentos no atendidos de coordinación con el fabricante. No cuentan con parche oficial al momento de la divulgación ("unpatched"). No se registra reporte de explotación masiva en el entorno real ni inclusión en el catálogo KEV de CISA.
- Versiones afectadas: Librería Kaltura HTML5 (mwEmbed / html5lib) en versiones v2.45, v2.103 y anteriores, así como múltiples ramas 2.x que mantengan expuesto el archivo mwEmbedLoader.php, afectando tanto a servidores locales como a la infraestructura CDN compartida.

Impacto potencial:

- Lectura y exfiltración de archivos confidenciales del sistema: Un atacante anónimo puede consultar archivos locales críticos, como local.ini, exponiendo en texto plano credenciales de base de datos, contraseñas administrativas, secretos de socios y claves API.
- Ejecución remota de código (RCE) y control total del servidor: Permite el despliegue de webshells en directorios web expuestos, otorgando al atacante la capacidad de ejecutar comandos arbitrarios con los privilegios del usuario del servidor web.
- Compromiso masivo en entornos multi-tenant y CDN: Debido a que el endpoint afectado también se encuentra expuesto en las plataformas y redes CDN compartidas de Kaltura, la vulnerabilidad afecta potencialmente a múltiples clientes y plataformas alojadas de forma concurrente.
- Persistencia y movimiento lateral en la red corporativa: El compromiso del servidor de aplicaciones faculta a los atacantes a establecer mecanismos de persistencia, alterar bases de datos o pivotar hacia otros activos internos de la organización.

Recomendaciones de mitigación:

1. Restricción o bloqueo del endpoint vulnerable en el perímetro: Configurar reglas en el WAF, proxy inverso o CDN para bloquear o deshabilitar completamente el acceso público al endpoint mwEmbedLoader.php donde el reproductor no sea estrictamente necesario.
2. Implementación de lista blanca (Allow-list) para ServiceUrl: Restringir el parámetro ServiceUrl para que únicamente acepte peticiones dirigidas a la URL de la API de backend legítima y rechazar explícitamente esquemas que no sean HTTP o HTTPS (como file://).
3. Filtrado de caracteres de salto de directorio en uiconf_id: Implementar reglas de inspección que rechacen solicitudes que contengan secuencias de salto de directorio (../), rutas absolutas o separadores de directorio dentro de uiconf_id.
4. Endurecimiento de directorios de caché y rotación de credenciales: Bloquear la ejecución de scripts PHP en todos los directorios destinados a almacenamiento de caché y rotar de manera urgente todas las credenciales, llaves de API y secretos almacenados en el archivo local.ini en caso de que el endpoint haya estado expuesto.

Prioridad: Crítica.

Ampliar información:

- https://kb.cert.org/vuls/id/308749
- https://thehackernews.com/2026/08/unpatched-kaltura-mwembed-flaws-could.html
- https://vitisecurity.com/kaltura-mwembed-deserialization-unpatched-flaws-lessons/
- https://hacklido.com/news/unpatched-kaltura-mwembed-flaws-could-let-remote-attackers-read-files-and-run-code
- https://www.theexploitdesk.tech/article/unpatched-kaltura-mwembed-flaws-could-let-remote-attackers-read-files--2de2bf

CISCO SECURE WORKLOAD – MÚLTIPLES VULNERABILIDADES CRÍTICAS PERMITEN EJECUCIÓN DE CÓDIGO Y EVASIÓN TOTAL DE CONTROLES (CVE-2026-20315 / CVE-2026-20317 / CVE-2026-20231 / CVE-2026-20318 / CVE-2026-20319)

Cisco ha publicado actualizaciones de seguridad para corregir cinco vulnerabilidades en la plataforma Cisco Secure Workload, afectando tanto a despliegues en la nube (SaaS) como a instalaciones locales (on-premises). Las fallas, identificadas durante revisiones internas de seguridad, incluyen problemas de control de acceso, elusión de autenticación e inyección de comandos, alcanzando severidades de hasta CVSS 10.0.

Resumen técnico:

- Identificador principal: CVE-2026-20315, CVE-2026-20317, CVE-2026-20231, CVE-2026-20318 y CVE-2026-20319.
- Severidad: Crítica (CVSS v3.1: 10.0 para CVE-2026-20315 y CVE-2026-20317; 9.9 para CVE-2026-20231; 9.6 para CVE-2026-20318; y 7.5/Alta para CVE-2026-20319).
- Causa raíz: Control de acceso inadecuado (CWE-284), autenticación incorrecta (CWE-287), neutralización inadecuada de elementos especiales e inyección (CWE-74), validación de entrada insuficiente (CWE-20) y gestión inadecuada de límites de memoria (CWE-119).
- Mecanismo de falla: La combinación de fallas permite a atacantes remotos con acceso de red inyectar comandos del sistema operativo y argumentos maliciosos, omitir mecanismos de validación de identidad y roles, manipular rutas del sistema de archivos (Path Traversal) y provocar desbordamientos de búfer mediante solicitudes manipuladas.
- Estado de explotación: Divulgadas oficialmente por Cisco el 20 y 21 de agosto de 2026. Fueron detectadas durante pruebas internas del fabricante y no se registra evidencia de explotación activa en el entorno real al momento de la publicación.
- Versiones afectadas: Cisco Secure Workload versiones 3.10 y anteriores, así como la rama 4.0.

Impacto potencial:

- Evasión total de autenticación y elevación de privilegios: Permite a atacantes no autenticados eludir los controles de acceso para ejecutar funciones administrativas no autorizadas dentro de la plataforma (CVE-2026-20315, CVE-2026-20317).
- Ejecución remota de código y comandos del sistema: La inyección de comandos y la manipulación de búferes de memoria facultan a los atacantes a ejecutar instrucciones arbitrarias con altos privilegios en el sistema anfitrión (CVE-2026-20231, CVE-2026-20319).
- Acceso y manipulación no autorizada del sistema de archivos: Mediante técnicas de salto de directorio (Path Traversal), se pueden leer, alterar o manipular recursos y archivos críticos dentro de la infraestructura (CVE-2026-20318).
- Compromiso de la visibilidad y segmentación de la red corporativa: El control no autorizado de la plataforma compromete las políticas de microsegmentación y la monitorización de seguridad en cargas de trabajo de la organización.

Recomendaciones de mitigación:

1. Actualización prioritaria de instancias on-premises: Aplicar de inmediato los parches oficiales para las ramas correspondientes: actualizar a la versión 3.10.9.1 (para versiones 3.10 y anteriores) o a la versión 4.0.4.16 (para la rama 4.0).
2. Actualización de componentes en la nube (SaaS): En despliegues SaaS, confirmar la actualización de las instancias locales de los agentes (Agent) y conectores (Connector), dado que el software central del clúster ya fue actualizado por Cisco.
3. Restricción y segmentación del acceso a la interfaz de gestión: Aislar las interfaces de administración de Cisco Secure Workload y limitar el acceso únicamente a subredes de confianza mediante reglas de firewall y listas de control de acceso (ACLs).
4. Monitoreo de registros de auditoría y telemetría de red: Monitorear activamente los logs de eventos del sistema en busca de patrones anómalos de solicitudes HTTP/API, intentos de salto de directorio o ejecuciones de comandos no autorizadas.

Prioridad: Crítica.

Ampliar información:

- https://www.euskadi.eus/gobierno-vasco/-/noticia/2026/cisco-corrige-multiples-vulnerabilidades-criticas-secure-workload/
- https://www.incibe.es/incibe-cert/alerta-temprana/avisos/multiples-vulnerabilidades-en-productos-de-cisco-12
- https://portal.cci-entel.cl/Threat_Intelligence/Boletines/2607
- https://www.moncloa.com/2026/08/22/incibe-cert-vulnerabilidades-productos-cisco-3419359/
- https://thehackernews.com/2026/08/cisco-patches-nine-crosswork-and-secure.html

SPLUNK ENTERPRISE Y COMPONENTES ADICIONALES – DESERIALIZACIÓN NO SEGURA Y FALLAS EN REST API PERMITEN EJECUCIÓN REMOTA DE CÓDIGO Y EXPOSICIÓN DE CREDENCIALES (CVE-2026-76404 / CVE-2026-76395 / CVE-2026-76402)

Splunk ha publicado un paquete de actualizaciones de seguridad urgente para corregir un conjunto de 17 vulnerabilidades que afectan a múltiples aplicaciones y complementos (add-ons) integrados en el entorno Splunk Enterprise, como Splunk MCP Server, Splunk AI Toolkit y Splunk Connect for Kafka. Las fallas de mayor impacto radican en la deserialización no segura de datos y la falta de validación en la API REST, permitiendo a usuarios con privilegios elevados o de rol "power" ejecutar comandos del sistema operativo (RCE) y exfiltrar claves o tokens de autenticación mediante solicitudes de falsificación del lado del servidor (SSRF).

Resumen técnico:

- Identificador principal: CVE-2026-76404 (Acompañado de CVE-2026-76395, CVE-2026-76391, CVE-2026-76394, CVE-2026-76402, entre otros listados en el aviso SVD-2026-0808).
- Severidad: Crítica (CVSS v3.1: 9.1 para CVE-2026-76404; CVSS v3.1: 8.8 a 8.2/Alta para los componentes de AI Toolkit y Kafka Connect).
- Causa raíz: Deserialización de datos no confiables (CWE-502), gestión inadecuada de privilegios, falta de autorización en endpoints REST API y Falsificación de Solicitudes del Lado del Servidor (SSRF).
- Mecanismo de falla: En Splunk MCP Server, una validación insuficiente de credenciales permite la deserialización de objetos maliciosos y la ejecución de comandos con el rol "admin". En Splunk AI Toolkit, modelos manipulados con matrices dispersas y código pickle embebido permiten ejecución remota de código. En Splunk Connect for Kafka, una vulnerabilidad SSRF en la API REST puede forzar conexiones a servidores externos para capturar credenciales del HTTP Event Collector (HEC).
- Estado de explotación: Divulgadas oficialmente por el fabricante en su boletín del 19 y 20 de agosto de 2026. No se registra reporte de explotación activa en el entorno real al momento de la publicación.
- Versiones afectadas: Splunk MCP Server en versiones anteriores a 1.2.1; Splunk AI Toolkit anterior a 6.0.0 (o 6.0.1 según la falla); Splunk Connect for Kafka anterior a 2.2.7; y Cisco Talos Intelligence for ES Cloud anterior a 1.0.3.

Impacto potencial:

- Ejecución remota de comandos en el sistema operativo anfitrión: Permite a usuarios autenticados con rol administrativo o de poder ejecutar instrucciones arbitrarias a nivel de servidor mediante la carga de modelos maliciosos o datos deserializados.
- Exfiltración de credenciales y tokens de autenticación: La explotación de fallos SSRF en Kafka Connect y Cisco Talos habilita la redirección de solicitudes a infraestructura controlada por atacantes, exponiendo claves API y tokens del HTTP Event Collector.
- Escalación de privilegios y manipulación del sistema: Fallas en la autorización de APIs REST del AI Toolkit facultan a usuarios con bajos privilegios a ejecutar búsquedas con permisos de nivel de sistema y tomar control no autorizado de contenedores.
- Interrupción de la continuidad operativa y denegación de servicio (DoS): Ataques mediante expresiones regulares o sobrecarga de reintentos en los conectores de eventos pueden provocar caídas de servicio e inestabilidad en el procesamiento de logs.

Recomendaciones de mitigación:

1. Actualización prioritaria de aplicaciones y add-ons: Actualizar de inmediato Splunk MCP Server a la versión 1.2.1, Splunk AI Toolkit a la versión 6.0.0/6.0.1, Splunk Connect for Kafka a la versión 2.2.7 y Cisco Talos Intelligence a la versión 1.0.3.
2. Deshabilitación temporal de componentes no parcheados: De no ser posible la actualización inmediata, deshabilitar o desinstalar el complemento Splunk MCP Server o el AI Toolkit en los servidores expuestos para cerrar el vector de RCE.
3. Restricción perimetral de interfaces administrativas y APIs: Restringir estrictamente el acceso a la API REST de Kafka Connect y a los paneles administrativos de Splunk únicamente a redes de gestión y direcciones IP autorizadas.
4. Auditoría de asignación de roles y permisos: Revisar exhaustivamente la asignación de privilegios administrativos ("admin" y "power") en la plataforma Splunk para reducir la superficie de exposición y detectar cuentas anómalas.

Prioridad: Crítica.

Ampliar información:

- https://ciberseguridad.cicese.mx/alerta/2703/Splunk-corrige-un-fallo-cr%C3%ADtico-en-Splunk-Enterprise-que-abre-la-puerta-a-ejecuci%C3%B3n-remota-de-c%C3%B3digo-sin-autenticaci%C3%B3n
- https://devel.group/blog/parches-urgentes-para-17-vulnerabilidades-en-splunk-ai-toolkit-kafka-connect-y-mcp-server/
- https://cyberpress.org/splunk-mcp-server-rce-ai-toolkit-vulnerabilities/
- https://www.cloudnetworks.co.kr/en/pr_en/blog/?mod=document&uid=435

MALWARE

SLEEPWALKER – PUERTA TRASERA PASIVA EN MEMORIA SE ACTIVA MEDIANTE UN ÚNICO PAQUETE DE RED CIFRADO Y LENGUAJE BYTECODE PROPIO

Investigadores de ciberseguridad han divulgado el hallazgo de SLEEPWALKER, una nueva y avanzada puerta trasera pasiva para sistemas Windows diseñada para permanecer inactiva en la memoria del sistema sin realizar conexiones salientes ni patrones de beaconing hacia servidores C2. El implante se enmascara como un componente legítimo del agente de administración de ESET y solo se activa tras recibir un único paquete de red cifrado ("magic packet") construido a medida, reduciendo drásticamente la huella en red y dificultando su detección por herramientas de seguridad convencionales.

Resumen técnico:

- Identificador principal: Implante pasivo SLEEPWALKER (DLL sustituta dpapi.dll / Hash SHA-256: d347170752a28e2b8c4b8b9f3cab2e3a6541ba11682c94498d26eb9002779d60).
- Tipo de amenaza: Puerta trasera para Windows (Windows Backdoor) residente en memoria, Implante pasivo post-compromiso y Motor de bytecode personalizado.
- Mecanismo de acceso e infección: Técnica de DLL Side-loading aprovechando el orden de búsqueda de Windows en el proceso ERAAgent.exe (ESET Management Agent). Requiere privilegios previos de administrador local para depositar la DLL maliciosa en el directorio del agente.
- Capacidades avanzadas y evasión: Ausencia total de direcciones IP/dominios hardcodeados o tráfico saliente periódico; cifrado de comandos mediante AES-256-CCM; ejecución de instrucciones a través de un lenguaje de bytecode propietario de 23 opcodes; monitoreo en modo promiscuo de la interfaz de red para capturar el paquete disparador; suplantación de metadatos de versión y exportación de funciones de la librería legítima dpapi.dll.
- Canales y transportes soportados: Soporta 6 vías de transporte para la recepción de comandos y entrega de cargas: TCP, UDP, ICMP, named pipes mediante SMB, sockets VMCI de VMware (comunicación directa huésped-hipervisor) y captura en modo promiscuo, además de un mecanismo latente basado en peticiones DNS.
- Mecanismos de persistencia: Carga automática mediante DLL Side-loading cada vez que se inicia el servicio ERAAgent.exe. Para facilitar el acceso no autenticado a sus named pipes, modifica las claves del registro EveryoneIncludesAnonymous y NullSessionPipes.
- Estado de actividad: Análisis técnico y reglas YARA divulgadas públicamente entre el 24 y el 26 de agosto de 2026 por el investigador Dominik Reichel. Corresponde a una amenaza post-compromiso altamente dirigida sin telemetría de infecciones masivas confirmadas en el entorno real.

Impacto potencial:

- Evasión avanzada de sistemas de inspección de red (NDR/IDS): Al no generar tráfico saliente hacia infraestructura C2 ni patrones de beaconing, la amenaza permanece invisible ante controles perimetrales y listas de reputación de dominios e IPs.
- Ejecución arbitraria de código y componentes maliciosos en memoria: Su motor de bytecode de 23 instrucciones permite interpretar tareas complejas, descargar etapas adicionales y ejecutar código binario directamente en la RAM sin dejar rastro en disco.
- Degradación de las directivas de seguridad del sistema operativo: La alteración de claves del registro de Windows (EveryoneIncludesAnonymous y NullSessionPipes) reduce las barreras de autenticación locales, facilitando el acceso anónimo y el movimiento lateral.
- Comunicaciones encubiertas e indetectables en entornos virtualizados: El uso de sockets VMCI permite establecer comunicaciones directas entre máquinas virtuales huéspedes y el servidor anfitrión ESXi, omitiendo firewalls y controles de tráfico en la red virtualizada.

Recomendaciones de mitigación:

1. Auditoría de integridad y detección de archivos anómalos en el agente ESET: Inspeccionar los directorios de instalación de ESET Management Agent (ERAAgent.exe) en busca de librerías dpapi.dll o dpapisvc.dll no autorizadas o discrepancias en los hashes de los archivos.
2. Monitoreo y restricción de modificaciones en el Registro de Windows: Implementar alertas en la solución EDR/SIEM ante cambios no autorizados en las claves EveryoneIncludesAnonymous (valor cambiado a 1) y modificaciones en la lista NullSessionPipes.
3. Endurecimiento de políticas de carga de DLL y control de aplicaciones: Aplicar políticas de AppLocker, Software Restriction Policies (SRP) o controles de integridad de código para impedir la ejecución de DLLs no firmadas o cargadas desde rutas no esperadas.
4. Detección de activación de modo promiscuo e inspección de tráfico Este-Oeste: Monitorear en los hosts la activación no autorizada de interfaces de red en modo promiscuo y reforzar la segmentación de red interna para detectar paquetes manipulados a nivel de tráfico local.

Prioridad: Urgente.

Ampliar información:

- https://unaaldia.hispasec.com/sleepwalker-introduce-una-puerta-trasera-para-windows-que-solo-despierta-con-un-unico-paquete-de-red/
- https://propakistani.pk/2026/08/25/new-windows-backdoor-can-hide-silently-until-hackers-activate-it/#google_vignette
- https://thehackernews.com/2026/08/newly-sleepwalker-backdoor-waits-for.html
- https://tech.yahoo.com/cybersecurity/articles/windows-malware-lays-dormant-until-161000667.html
- https://www.scworld.com/brief/new-sleepwalker-backdoor-uses-custom-command-language-remains-hidden

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

GITEA – EXPLOTACIÓN ACTIVA DE VULNERABILIDAD CRÍTICA DE INYECCIÓN DE CÓDIGO Y RCE VÍA ENDPOINT DIFFPATCH (CVE-2026-60004)

La Agencia de Ciberseguridad e Infraestructura de EE. UU. (CISA) ha añadido a su catálogo de Vulnerabilidades Explotadas Conocidas (KEV) el fallo crítico CVE-2026-60004 en Gitea, la popular plataforma de gestión de repositorios Git de código abierto. La vulnerabilidad permite a un atacante con acceso de escritura en un repositorio ejecutar comandos de shell arbitrarios con los privilegios de la cuenta de servicio de Gitea. El riesgo se agrava drásticamente debido a que la configuración predeterminada de Gitea mantiene el registro abierto a nuevos usuarios, permitiendo que atacantes anónimos obtengan permisos de escritura sin credenciales previas para desplegar campanas de cryptojacking y minería no autorizada de criptomonedas.

Resumen técnico:

- Identificador principal: CVE-2026-60004.
- Severidad: Crítica (CVSS v3.1: 9.8 / Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).
- Causa raíz: Inyección de código (CWE-94) por procesamiento y validación inadecuada de parches en el endpoint de API /diffpatch.
- Mecanismo de falla: Un atacante con permisos de escritura envía un parche malicioso manipulado al endpoint API diffpatch, logrando inyectar un Git hook ejecutable dentro del directorio .git/hooks/ del repositorio. Cuando se activan operaciones Git posteriores, el script malicioso se ejecuta automáticamente en el sistema operativo anfitrión con los privilegios del proceso de Gitea.
- Estado de explotación: Confirmada explotación activa en el entorno real e incluida oficialmente en el catálogo KEV de CISA el 25 de agosto de 2026. Se registran ataques activos orientados al despliegue de droppers que eliminan procesos competidores y consumen masivamente la CPU del servidor para minería no autorizada.
- Versiones afectadas: Gitea desde la versión 1.17 hasta versiones anteriores a 1.27.0 (corregido oficialmente en la versión 1.27.1).

Impacto potencial:

- Ejecución remota de código (RCE) y control del servidor anfitrión: Un atacante puede ejecutar instrucciones arbitrarias a nivel de sistema operativo bajo el contexto del usuario de servicio de Gitea, abriendo la puerta al control total del sistema.
- Evasión de autenticación vía registro abierto predeterminado: La combinación de la vulnerabilidad con la configuración por omisión (DISABLE_REGISTRATION = false) permite a atacantes externos registrarse, crear repositorios y obtener permisos de escritura de forma anónima sin requerir credenciales previas.
- Despliegue de malware y saturación de recursos por Cryptojacking: Los ataques activos aprovechan la ejecución de comandos para instalar droppers que detienen procesos del sistema y consumen más del 70% de la capacidad de CPU para minar criptomonedas.
- Riesgo para la cadena de suministro (Supply Chain) y exfiltración de código: Al tomar el control de la plataforma de desarrollo, el atacante puede exfiltrar repositorios privados, acceder a secretos o inyectar código malicioso en los pipelines de integración continua (CI/CD).

Recomendaciones para mitigar el riesgo:

1. Actualización prioritaria a la versión corregida: Actualizar de forma urgente todas las instancias autogestionadas de Gitea a la versión 1.27.1 o superior para eliminar el fallo en la API.
2. Deshabilitación del registro abierto (Mitigación temporal inmediata): En caso de no poder parchear inmediatamente, modificar el archivo de configuración app.ini estableciendo DISABLE_REGISTRATION = true para restringir la creación de cuentas únicamente a administradores.
3. Endurecimiento de políticas de acceso y autenticación: Configurar REQUIRE_SIGNIN_VIEW = true, habilitar REGISTER_EMAIL_CONFIRM = true y desactivar ENABLE_OPENID_SIGNUP para evitar que bots o usuarios anónimos interactúen con las APIs.
4. Auditoría de Git hooks y monitoreo de procesos anómalos: Inspeccionar los directorios .git/hooks/ en los repositorios de la instancia en busca de scripts sospechosos recién creados, y auditar los registros de consumo de CPU e interacciones con el endpoint diffpatch.

Prioridad: Urgente.

Ampliar Información:

- https://thehackernews.com/2026/08/critical-gitea-rce-actively-exploited.html
- https://www.ciberplaneta.org/vulnerabilidades/cve-2026-60004-vulnerabilidad-critica-de-inyeccion-de-codigo-en-gitea-explotada-activamente/
- https://blog.elhacker.net/2026/08/alerta-por-vulnerabilidad-critica-de.html
- https://cybersecurefox.com/es/cve-2026-60004-vulnerabilidad-critica-gitea/
- https://www.runzero.com/blog/gitea/