GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °4126

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

BOLETÍN CIBERSEGURIDAD
SEMANAL EDICIÓN °4126

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 CE/EE – VULNERABILIDAD CRÍTICA DE DESBORDAMIENTO DE ENTERO EN COMPILADOR DE REGEX DE CI/CD PERMITE EJECUCIÓN REMOTA DE CÓDIGO (CVE-2026-97229)

GitLab ha publicado un aviso de seguridad y parches de actualización urgente para corregir una vulnerabilidad de severidad crítica en el compilador de expresiones regulares del motor de CI/CD. La falla se debe a un desbordamiento de entero (Integer Overflow) en el motor de expresiones regulares Onigmo utilizado por Ruby. Bajo ciertas condiciones, un usuario sin autenticación o con permisos para publicar en un proyecto público puede lograr la ejecución arbitraria de código (RCE) en el servidor subyacente de GitLab mediante una configuración de CI/CD (.gitlab-ci.yml) manipulada que evalúe rutas de repositorio con caracteres UTF-8.

Resumen técnico:

- Identificador principal: CVE-2026-97229.
- Severidad: Crítica (CVSS v3.1: 10.0 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).
- Causa raíz: Desbordamiento de entero o envolvente (Integer Overflow or Wraparound - CWE-190) e insuficiente validación de expresiones regulares en el compilador de CI/CD.
- Mecanismo de falla: Un atacante deposita un archivo de configuración .gitlab-ci.yml con una expresión regular especialmente manipulada y una ruta de repositorio conteniendo caracteres UTF-8 en una rama de un proyecto público.
- La expresión regular se compila inicialmente en representación US-ASCII compacta superando las validaciones iniciales de la aplicación.
- Al evaluarse contra la ruta UTF-8, el motor Onigmo recompila la expresión; un desbordamiento de entero en el cálculo del tamaño del programa genera instrucciones de regex inválidas, provocando la pérdida de integridad en el flujo de control.
- Esto permite ejecutar operaciones arbitrarias en la máquina virtual de Onigmo dentro del proceso de Ruby, derivando en la ejecución de comandos del sistema operativo con los privilegios del usuario git.
- Estado de explotación: Divulgada oficialmente el 12 de octubre de 2026. No se registra confirmación de explotación activa masiva en el entorno real, pero existe una prueba de concepto (PoC) pública funcional desarrollada por Rapid7 que confirma la ejecución remota de código en instancias sin parchear.
- Versiones afectadas: GitLab CE/EE autoalojado en todas las versiones desde la 19.2 anteriores a 19.2.8, 19.3 anteriores a 19.3.5, y 19.4 anteriores a 19.4.2. (Las plataformas gestionadas GitLab.com y GitLab Dedicated fueron corregidas previamente).

Impacto potencial:

- Ejecución remota de código (RCE) no autorizada: Otorga a un atacante la capacidad de ejecutar comandos arbitrarios a nivel de sistema operativo en el servidor de GitLab bajo el contexto del usuario del sistema git.
- Compromiso total del código fuente y repositorios: Facilita el acceso no autorizado, exfiltración, modificación o eliminación de repositorios y proyectos almacenados en la instancia.
- Exfiltración masiva de secretos y variables de CI/CD: Permite la extracción de tokens de acceso a la API, claves de despliegue (deploy keys), credenciales de infraestructura en la nube y variables de entorno protegidas.
- Movimiento lateral hacia la cadena de suministro: Habilita el pivoteo desde el servidor de GitLab hacia los ejecutores (GitLab Runners), permitiendo contaminar canalizaciones de despliegue e infectar entornos de producción.

Recomendaciones de mitigación:

1. Actualización prioritaria de instancias autoalojadas: Desplegar de forma inmediata las versiones corregidas de GitLab CE/EE 19.2.8, 19.3.5 o 19.4.2 (evitando la versión 19.3.4 por problemas conocidos de integración).
2. Restricción del registro de usuarios y proyectos públicos: Deshabilitar la funcionalidad de autorregistro público (self-registration) y restringir los permisos de creación o escritura en proyectos públicos a usuarios de estricta confianza.
3. Auditoría de repositorios y configuraciones de CI/CD: Inspeccionar las cuentas creadas a partir del 12 de octubre de 2026 y auditar archivos .gitlab-ci.yml en proyectos públicos que incluyan expresiones regulares complejas o rutas con caracteres UTF-8 inusuales.
4. Monitoreo y caza de amenazas (Threat Hunting): Implementar reglas en EDR/SIEM para detectar la creación de procesos secundarios inusuales generados desde los servicios de GitLab, monitorear caídas anómalas en trabajadores de ci lint/workhorse, y verificar la adición no autorizada de runners, hooks o tokens.

Prioridad: Crítica.

Ampliar información:

- https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-4-2-released/
- https://www.helpnetsecurity.com/2026/10/13/gitlab-ci-cd-regular-expression-compiler-vulnerability-cve-2026-97229/
- https://thehackernews.com/2026/10/gitlab-patches-cvss-100-flaw-that-could.html
- https://www.rapid7.com/blog/post/etr-cve-2026-97229-critical-unauthenticated-remote-code-execution-in-gitlab/
- https://ciberseguridad.blog/gitlab-rce-critica-cvss-10-parche/

CITRIX NETSCALER ADC Y GATEWAY – VULNERABILIDAD CRÍTICA DE DESBORDAMIENTO DE MEMORIA EN SAML PERMITE EJECUCIÓN REMOTA DE CÓDIGO Y DENEGACIÓN DE SERVICIO (CVE-2026-107406)

Citrix ha publicado un aviso de seguridad (CTX697191) para corregir una vulnerabilidad de severidad crítica por desbordamiento de memoria (Memory Overflow) en NetScaler ADC y NetScaler Gateway configurados con funcionalidades de autenticación SAML. La falla permite a un atacante remoto no autenticado enviar peticiones o comunicaciones especialmente manipuladas a través de la red para provocar la ejecución remota de código (RCE) arbitrario o causar una condición de denegación de servicio (DoS) en la infraestructura perimetral.

Resumen técnico:

- Identificador principal: CVE-2026-107406

(Boletín CTX697191 / Alerta INCIBE-2026-725).

- Severidad: Crítica

(CVSS v4.0: 9.5 Vector: CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:L).

- Causa raíz: Restricción inadecuada de operaciones dentro de los límites de un búfer de memoria (Improper Restriction of Operations within the Bounds of a Memory Buffer - CWE-119).
- Mecanismo de falla:
- Un atacante remoto sin autenticación transmite peticiones HTTP/S manipuladas hacia los puntos de enlace de autenticación SAML del dispositivo.
- La aplicación falla en validar correctamente los límites de memoria al procesar las solicitudes SAML, generando un desbordamiento en el búfer.
- La corrupción de memoria resultante permite desviar el flujo de ejecución para ejecutar código con privilegios elevados o colapsar los servicios de red.
- Estado de explotación: Divulgada oficialmente el 8 y 9 de octubre de 2026. No se registra confirmación de explotación activa no mitigada en el entorno real ni disponibilidad de exploit PoC público al momento de la publicación. CISA emitió una alerta recomendando la actualización inmediata por el alto riesgo que representan estos equipos perimetrales.
- Versiones afectadas: Instancias autoalojadas de NetScaler ADC y Gateway configuradas como SAML IdP (ramas 14.1 entre 14.1-73.37 y 14.1-73.41; 13.1 entre 13.1-64.23 y 13.1-64.28, y sus versiones FIPS/NDcPP equivalentes); versiones anteriores a 14.1-73.37 y 13.1-64.23 configuradas como SAML SP o IdP; e implementaciones híbridas de Citrix Secure Private Access. (Los servicios administrados en la nube por Citrix fueron actualizados automáticamente).

Impacto potencial:

- Ejecución remota de código (RCE) no autorizada: Otorga a un atacante la capacidad de ejecutar comandos arbitrarios con altos privilegios en el sistema operativo del appliance NetScaler.
- Denegación de servicio (DoS) en accesos perimetrales: Permite forzar caídas del servicio o reinicios del dispositivo, interrumpiendo el acceso remoto corporativo y la entrega de aplicaciones.
- Compromiso de credenciales y tokens SAML: Al actuar como Proveedor de Identidad (IdP) o de Servicios (SP), su vulneración expone secretos de sesión, tokens de autenticación y credenciales corporativas.
- Movimiento lateral hacia la red interna: Facilita el pivoteo directo desde el perímetro de la red (DMZ) hacia la infraestructura crítica y sistemas internos protegidos.

Recomendaciones de mitigación:

1. Actualización inmediata de firmware: Actualizar con urgencia los dispositivos afectados a las versiones corregidas 13.1-64.29, 14.1-73.46 FIPS o 13.1-37.283 FIPS/NDcPP (o posteriores).
2. Auditoría de la configuración SAML: Revisar el archivo de configuración para identificar si el equipo actúa como SAML SP (add authentication samlAction) o SAML IdP (add authentication samlIdPProfile) y determinar su nivel de exposición.
3. Centralización de registros y monitoreo (SIEM): Reenviar la telemetría y los registros de NetScaler hacia un SIEM o servidor syslog centralizado antes de aplicar parches, evitando la pérdida de evidencias forenses por rotación local de logs.
4. Caza de amenazas y respuesta ante sospecha de compromiso: Si se sospecha de un compromiso previo, preservar evidencia forense, restaurar respaldos seguros anteriores a la fecha del incidente y realizar una rotación obligatoria de certificados SSL, claves de cifrado y contraseñas locales.

Prioridad: Crítica.

Ampliar información:

- https://support.citrix.com/external/article/CTX697191/citrix-netscaler-adc-and-citrix-netscale.html
- https://thehackernews.com/2026/10/citrix-patches-critical-netscaler-flaw.html
- https://www.cisa.gov/news-events/alerts/2026/09/27/critical-zero-day-vulnerabilities-exploited-citrix-netscaler-adc-gateway
- https://socprime.com/blog/cve-2026-107406-critical-netscaler-rce-flaw/
- https://www.incibe.es/incibe-cert/alerta-temprana/avisos/desbordamiento-de-memoria-en-netscaler-adc-y-netscaler-gateway-de-citrix

SPLUNK ENTERPRISE Y SPLUNK SECURE GATEWAY – MÚLTIPLES VULNERABILIDADES CRÍTICAS Y ALTAS PERMITEN EJECUCIÓN REMOTA DE COMANDOS Y ESCALADA DE PRIVILEGIOS (CVE-2026-76268, CVE-2026-76266 Y OTROS)

Splunk ha emitido un aviso de seguridad (SVD-2026-1001) para abordar múltiples vulnerabilidades en Splunk Enterprise y Splunk Secure Gateway. La falla más severa (CVE-2026-76268) se debe a la ausencia de autenticación en la API REST de Patroni del sidecar de PostgreSQL en miembros de clústeres de búsqueda (search head cluster members). Esto permite a un atacante remoto no autenticado con acceso a la red ejecutar comandos arbitrarios a nivel de sistema operativo con los privilegios del proceso de Splunk. Además, se corrigió una falla de escalada local de privilegios a root durante actualizaciones de paquetes en Linux (CVE-2026-76266) junto con múltiples fallas de control de acceso y derivación de autorización.

Resumen técnico:

- Identificador principal: CVE-2026-76268 (Aviso SVD-2026-1001 / Alerta INCIBE-2026-716).
- 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: Falta de autenticación para funciones críticas (Missing Authentication for Critical Function - CWE-306) en la API REST de Patroni, e inclusión no confiable de archivos durante actualizaciones de paquetes Linux (CWE-269).
- Mecanismo de falla:
- En CVE-2026-76268, la interfaz de la API REST de Patroni (asociada al sidecar de PostgreSQL) en miembros de clústeres de búsqueda no requiere autenticación para operaciones de configuración críticas. Un atacante envía solicitudes manipuladas a la API REST sin credenciales para ejecutar comandos del sistema operativo.
- En CVE-2026-76266, el script del mantenedor de paquetes Linux confía en archivos preexistentes del directorio de instalación al ejecutarse con privilegios root durante una actualización, permitiendo a un usuario local ejecutar comandos con máximos privilegios.
- Múltiples endpoints en Splunk Secure Gateway carecen de validación de autorización previa, permitiendo a usuarios con privilegios bajos firmar payloads no autorizados o manipular colecciones KV Store.
- Estado de explotación: Divulgada oficialmente el 7 de octubre de 2026. No se registra confirmación de explotación activa masiva en el entorno real al momento de la publicación. Existen repositorios con pruebas de concepto (PoC) públicas disponibles.
- Versiones afectadas: Splunk Enterprise ramas 10.4 (10.4.0 a 10.4.2), 10.2 (10.2.0 a 10.2.6), 10.0 (10.0.0 a 10.0.9) y 9.4 (9.4.0 a 9.4.14); y Splunk Secure Gateway en versiones anteriores a 3.10.11, 3.9.25 y 3.8.72. (Nota: CVE-2026-76268 solo afecta a las ramas 10.4.x y 10.2.x).

Impacto potencial:

- Ejecución remota de comandos (RCE) sin autenticación: Permite a un atacante remoto ejecutar comandos arbitrarios en el servidor del miembro del clúster de búsqueda sin requerir credenciales.
- Escalada local de privilegios a nivel de superusuario (Root LPE): Un usuario local con permisos del servicio Splunk puede tomar control total del sistema operativo subyacente con privilegios root durante la actualización del paquete Linux.
- Exposición y acceso no autorizado a información de búsquedas: Permite a usuarios de bajos privilegios acceder a consultas, metadatos y resultados de trabajos de búsqueda de otros usuarios (CVE-2026-76269 / CVE-2026-76275).
- Falsificación de firmas y alteración de datos en Splunk Secure Gateway: Posibilita firmar cargas manipuladas y alterar colecciones de KV Store utilizadas en flujos de alertas y dispositivos móviles (CVE-2026-76265 / CVE-2026-76280).

Recomendaciones de mitigación:

1. Actualización prioritaria a versiones de firmware corregidas: Actualizar Splunk Enterprise a las versiones 10.4.3, 10.2.7, 10.0.10 o 9.4.15 (según la rama utilizada) y Splunk Secure Gateway a 3.10.11, 3.9.25 o 3.8.72.
2. Deshabilitación del sidecar de PostgreSQL (Mitigación temporal CVE-2026-76268): Si no se puede actualizar de inmediato y no se utilizan Edge Processor, OpAmp o flujos de datos SPL2, deshabilitar el sidecar agregando disabled = true en la sección [postgres] del archivo $SPLUNK_HOME/etc/system/local/server.conf reiniciar el servicio.
3. Ajuste de configuración adicional post-actualización (CVE-2026-76264): Tras la actualización, configurar scripted_lookup_raw_write_enforcement = block dentro de la sección [lookup] en el archivo limits.conf y reiniciar Splunk Enterprise para bloquear la creación no autorizada de búsquedas con scripts.
4. Restricción de red y desactivación de aplicaciones no utilizadas: Segmentar y bloquear el acceso a la API REST de Patroni a nivel de red, y deshabilitar o remover la app Splunk Secure Gateway o la app de Observability Cloud si la organización no requiere sus funcionalidades.

Prioridad: Crítica.

Ampliar información:

- http://advisory.splunk.com/advisories/SVD-2026-1001
- https://ccb.belgium.be/advisories/warning-multiple-vulnerabilities-splunk-enterprise-including-critical-rce-patch
- https://csirt.telconet.net/comunicacion/boletines-servicios/splunk-enterprise-presenta-vulnerabilidad-critica-de-ejecucion-remota-de-comandos-sin-autenticacion/
- https://www.incibe.es/incibe-cert/alerta-temprana/avisos/multiples-vulnerabilidades-en-productos-de-splunk
- https://horizon3.ai/attack-research/vulnerabilities/cve-2026-76268/

MALWARE

CAMPAÑA POELLM (CANTO INCOGNITO) – MALWARE BASADO EN POESÍA ADVERSARIAL EXPLOTA INFRAESTRUCTURA DE INTELIGENCIA ARTIFICIAL PARA EXPANDIR BOTNET DE CRIPTOMINERÍA

Investigadores de ciberseguridad de Black Lotus Labs (división de Lumen) han documentado la campaña denominada Canto Incognito, la cual despliega una nueva familia de malware conocida como PoeLLM. Esta amenaza está dirigida contra servidores que albergan servicios y modelos de inteligencia artificial (IA/LLM) expuestos en Internet, tales como LiteLLM y Ollama, además de entornos adyacentes como Gotenberg y Gitea. El malware utiliza una técnica novedosa bautizada como "poesía adversarial" para extraer dinámicamente la dirección IP de su servidor de comando y control (C2) desde un poema alojado en GitHub, con el objetivo principal de secuestrar la capacidad de cómputo (GPU/CPU) para propagarse y minar la criptomoneda Monero mediante herramientas como XMRig.

Resumen técnico:

- Identificador principal: Campaña Canto Incognito / Malware PoeLLM (módulo ejecutable ELF libgcrypt).
- Tipo de amenaza: Botnet de minería de criptomonedas (Cryptominer) / Escáner de vulnerabilidades / Troyano / Amenaza a la infraestructura de IA.
- Mecanismo de acceso e infección:
- Explotación de vulnerabilidades conocidas en servicios de IA y aplicaciones expuestas a Internet. Destaca el encadenamiento de la falla de SSRF en endpoints de prueba MCP de LiteLLM (CVE-2026-42271) con la omisión de autenticación (CVE-2026-48710) para lograr ejecución remota de código (RCE) no autenticada.
- Extracción dinámica de C2 mediante "Poesía Adversarial": Tras la infección, PoeLLM descarga un archivo (dash.css) en un repositorio de GitHub que contiene un poema generado por IA titulado "On the Nature of Connection". Extrae palabras clave específicas (driver, diode, decryption, tick) y las traduce a valores numéricos usando un diccionario estático incorporado en su código para generar la dirección IPv4 del servidor C2.
- Flexibilidad operativa: El operador modifica el poema publicado en GitHub (actualizado al menos 11 veces) para cambiar la IP de mando y control, haciendo que los equipos infectados recalculen la nueva dirección sin necesidad de redistribuir el malware.
- Estado de actividad: Detectado y rastreado activamente en octubre de 2026. Ha infectado a más de 3,400 servidores (principalmente en EE. UU. y Europa Occidental), alcanzando picos de 800 sistemas infectados activos simultáneamente en un solo día.
- Plataformas afectadas: Servidores con infraestructura de IA y servicios expuestos en Internet (LiteLLM, Ollama, convertidor de PDF Gotenberg, Gitea y endpoints de Ivanti Sentry).

Impacto potencial:

- Secuestro masivo de recursos de cómputo (Resource Hijacking): Consumo intensivo y no autorizado de la capacidad de procesamiento de CPU y clústeres de GPU para minar Monero mediante los mineros XMRig e Iron conectados a servicios como Kryptex.
- Propagación lateral y expansión de la botnet: Conversión del servidor comprometido en un nodo escáner activo que rastrea los puertos 3000 y 4000 para localizar y explotar otros servicios de IA vulnerables en la red corporativa o en Internet.
- Exposición y exfiltración de datos de modelos de IA: Riesgo de acceso no autorizado a datos de entrenamiento, consultas procesadas por los modelos de lenguaje, claves de API, tokens de autenticación y recursos internos de la red.
- Degradación del servicio y sobrecostos en infraestructura cloud: Interrupción operativa de los servicios de IA corporativos y disparos severos en la facturación de servicios en la nube debido al uso ininterrumpido de procesamiento de alto rendimiento.

Recomendaciones de mitigación:

1. Actualización prioritaria de servicios de IA: Aplicar parches de forma inmediata en las instancias de LiteLLM (actualizando a versiones 1.47.4 o superiores) para corregir CVE-2026-42271 y CVE-2026-48710, además de actualizar Ollama, Gotenberg y Gitea.
2. Segmentación de red y políticas de filtrado saliente (Egress Control): Implementar arquitectura Zero Trust para aislar los entornos de IA de la Internet pública y configurar reglas en cortafuegos/WAF para bloquear conexiones hacia dominios de mining pools (como Kryptex) e IP no autorizadas.
3. Monitoreo de rendimiento y telemetría de red: Establecer alertas ante picos inusuales de uso en CPU/GPU y supervisar el tráfico saliente en busca de consultas sospechosas a repositorios de GitHub o patrones de escaneo en los puertos 3000 y 4000.
4. Auditoría de credenciales y hardening de IA: Deshabilitar la exposición pública de servicios de IA sin autenticación robusta, revisar claves de API/tokens de acceso y realizar rotación inmediata de credenciales en los servidores afectados o sospechosos.

Prioridad: Urgente.

Ampliar información:

- https://www.infobae.com/tecno/2026/10/08/ciberdelincuentes-usan-un-poema-para-infectar-miles-de-servidores-con-malware/
- https://www.forgenex.com/blog/poellm-malware-ataca-3-400-servidores-de-ia-para-minar-criptomonedas
- https://www.elcomercio.com/tecnologia/ciberseguridad-malware-servidores-virus/
- https://aviatrix.ai/threat-research-center/poellm-malware-cryptomining-attacks-ai-servers-2026/
- https://blog.elhacker.net/2026/10/malware-poellm-ataca-servidores-de-ia.html

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.

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

BOLETÍN CIBERSEGURIDAD
SEMANAL EDICIÓN °4126

NOTICIAS DE CIBERSEGURIDAD

ATAQUES CONTRA IVANTI CONNECT SECURE – EXPLOTACIÓN ENCADENADA DE VULNERABILIDADES DE DÍA CERO PERMITE EJECUCIÓN REMOTA DE CÓDIGO CON PRIVILEGIOS DE ROOT (CVE-2026-104935)

Investigadores de ciberseguridad y el fabricante Ivanti han alertado sobre la explotación activa en el entorno real de una cadena de vulnerabilidades de día cero (Zero-Day) en la pasarela VPN corporativa Ivanti Connect Secure (ICS). Identificada inicialmente por la firma Volexity como parte de las acciones del actor de amenazas UTA0576, la campaña combina una omisión de autenticación y una ejecución remota de código (RCE) —rastreadas bajo el identificador CVE-2026-104935— junto con un fallo de escalada de privilegios aún no parcheado para tomar el control total de los dispositivos a nivel root sin requerir credenciales previas.

Resumen técnico:

- Identificador principal: Cadena de Zero-Days en Ivanti Connect Secure (CVE-2026-104935 / Alerta CISA KEV / Volexity UTA0576).
- Tipo de amenaza: Explotación de vulnerabilidades de día cero (Zero-Day) / Omisión de autenticación / Ejecución remota de código (RCE) / Escalada de privilegios a Root.
- Modo de operación:
- El atacante transmite solicitudes HTTP no autenticadas hacia /dana-na/auth/url_default/welcome.cgi incluyendo la cabecera X-DSCGI-PATH para redirigir la petición hacia scripts CGI protegidos internos (como wu.cgi).
- Explota una condición de carrera al subir un script en formato ZIP que ejecuta código Python directamente en la memoria del sistema antes de que el manejador de la aplicación lo elimine del disco.
- Eleva privilegios a root parcheando en memoria la librería /home/lib/libdsplibs.so para alterar el servicio dsinvoked, ejecutando comandos posteriores mediante peticiones HTTPS repetidas sin instalar web shells o backdoors permanentes en disco.
- Realiza técnicas antiforenses eliminando registros en /home/runtime/dlogs/debuglog y /var/log/audit/audit.log, restaurando el estado de la memoria para evadir la herramienta de verificación de integridad (Integrity Checker Tool) de Ivanti.

- Estado de actividad: Confirmada en explotación activa masiva en el entorno real como vulnerabilidad de día cero desde al menos el 1 de octubre de 2026; incluida en el catálogo KEV de la CISA.
- Versiones afectadas: Ivanti Connect Secure (ICS) en versiones 22.8R2.4 y anteriores, 25.1.2.2 y anteriores, y 25.1.1.1 y anteriores. (Las versiones 25.1.3.0, 25.1.3.1, 22.8R2.5 y 22.7R2.14 figuran como no afectadas por la parte corregida).

Impacto potencial:

- Control total del dispositivo perimetral a nivel Root: Otorga ejecución remota de código no autenticada con máximos privilegios administrativos, permitiendo tomar el control absoluto del sistema operativo de la pasarela VPN.
- Extracción masiva de credenciales y metadatos de Active Directory: Facilita la exfiltración de contraseñas de dominio, credenciales de administración local (LAPS), claves de recuperación de BitLocker y atributos de usuario mediante herramientas LDAP y Kerberos personalizadas.
- Intercepción de tráfico y captura no autorizada de paquetes: Permite ejecutar herramientas de captura de red (tcpdump / dsstatmond) ocultas en el directorio .icscap para capturar tráfico en puertos sensibles (como LDAP/TCP 389) y extraer credenciales en texto plano o hashes NTLM.
- Reconocimiento interno y preparación para movimiento lateral: Habilita la realización de ataques de password spraying, resolución de nombres de la red interna y escaneo de servicios corporativos para preparar la intrusión hacia la infraestructura interna.

Recomendaciones para mitigar el riesgo:

- Actualización prioritaria del firmware de Ivanti Connect Secure: Desplegar de inmediato los parches emitidos por el fabricante (versiones 25.1.3.0, 25.1.3.1, 22.8R2.5 o superiores) para corregir los componentes de omisión de autenticación y RCE.
- Caza de amenazas e inspección de indicadores de compromiso (IoC): Auditar los registros del servidor web en busca de solicitudes frecuentes a /dana-na/auth/url_default/welcome.cgi con la cabecera X-DSCGI-PATH, revisar la presencia del directorio oculto /data/.icscap/ y monitorear conexiones hacia la IP 108.165.147[.]64.
- Análisis forense de red y memoria: Debido a que el exploit modifica el código únicamente en memoria y limpia los registros para evadir la herramienta Integrity Checker Tool (ICT), realizar adquisiciones de memoria volátil e inspección profunda de tráfico si se sospecha de un compromiso.
- Aislamiento y rotación obligatoria de credenciales: En caso de confirmar la vulneración, aislar la pasarela VPN, restaurar una copia de respaldo limpia previa al incidente y rotar las credenciales de Active Directory, cuentas LDAP, claves criptográficas y contraseñas LAPS expuestas.

Prioridad: Urgente.

Ampliar Información:

- https://thehackernews-com.translate.goog/2026/10/attacker-chains-three-ivanti-connect.html?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc
- https://ciberseguridadegalicia.gal/es/ciberseguridad-al-dia/alertas/alerta-por-explotacion-activa-de-una-vulnerabilidad-zero-day-en-ivanti-connect-secure
- https://www-volexity-com.translate.goog/blog/2026/10/13/a-series-of-unauthenticated-events-chained-exploitation-of-ivanti-connect-secure-zero-days/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc
- https://www-rapid7-com.translate.goog/blog/post/etr-ivanti-connect-secure-zero-day-exploited-in-the-wild-cve-2026104935/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc&_x_tr_hist=true
- https://www-bleepingcomputer-com.translate.goog/news/security/ivanti-warns-of-connect-secure-zero-day-exploited-in-attacks/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc