



RADAR CTI

BOLETÍN SEMANAL
DE CIBERSEGURIDAD

INTELIGENCIA PARA ANTICIPARNOS HOY, PROTEGER TU MAÑANA.

Análisis, contexto y acciones concretas sobre las
amenazas más relevantes de la semana.



AMENAZAS
EN LA MIRA



VULNERABILIDADES
CRÍTICAS



INCIDENTES
RELEVANTES



ACCIONES
INMEDIATAS

VULNERABILIDAD CRÍTICA / BACKUP

AhsayCBS: RCE explotada contra la infraestructura de backup

AHSAYCBS RCE WEBSHELL XMRIG

**QUÉ ESTÁ PASANDO**

Huntress observó la explotación encadenada de CVE-2026-105133 y CVE-2026-105134 en AhsayCBS. El acceso permitió ejecutar código sin autenticación y desplegar webshells JSP y XMRig; ya había cinco organizaciones afectadas al 8 de Octubre.

POR QUÉ IMPORTA

AhsayCBS concentra la administración de respaldos y suele estar conectado a múltiples clientes cuando lo opera un MSP o integrador. Comprometerlo puede dar una posición privilegiada sobre recuperación y continuidad de negocio.

QUÉ REVISAR AHORA

- Identificar AhsayCBS expuestos y restringir su administración.
- Confirmar versión; Huntress considera afectadas hasta 10.3.4.
- Buscar cbssvcX64.exe → curl/certutil y webshells JSP.
- Buscar XMRig, MicrosoftEdgeUpdateSvc y WinRing0x64.sys.

PERÍMETRO / VPN

SonicWall SMA1000: CVE crítica de SSRF y señales de explotación

SONICWALL SMA1000 CVSS 10

**QUÉ ESTÁ PASANDO**

SonicWall publicó el CVE-2026-102255, CVSS 10.0, una SSRF preautenticada en SMA1000. El proveedor inicialmente indicó no tener evidencia de explotación; el Canadian Cyber Centre reportó el 7 de Octubre que fuentes abiertas indicaban explotación in the wild.

POR QUÉ IMPORTA

SMA1000 está en el perímetro y expuesto para acceso remoto. La diferencia entre la evaluación inicial del proveedor y la evidencia posterior hace que la revisión de exposición y logs sea prioritaria.

QUÉ REVISAR AHORA

- Identificar SMA1000 6210, 7210 y 8200v expuestos.
- Actualizar a 12.4.3-03670+ o 12.5.0-03082+.
- Revisar logs de WorkPlace y solicitudes anómalas.
- Revisar cambios administrativos posteriores al 7 de Octubre.

COLLABORATION / DEVOPS

Atlassian Data Center: acceso arbitrario a archivos en ocho productos

ATLASSIAN CVE-2026-21589 CVSS 9.3

**QUÉ ESTÁ PASANDO**

Atlassian publicó el CVE-2026-21589, una falla de acceso arbitrario a archivos en Bitbucket, Confluence, Jira, JSM, Bamboo, Crowd, Crucible y Fisheye Data Center. Requiere conocer el nombre y ruta exactos del archivo; no permite listar directorios.

POR QUÉ IMPORTA

Los productos pueden contener configuración, código y archivos con información sensible. Atlassian no confirmó explotación y Censys tampoco reportó explotación pública al 7 de Octubre, pero las instancias públicas deben tratarse como prioridad.

QUÉ REVISAR AHORA

- Inventariar todos los productos Data Center expuestos.
- Aplicar versiones corregidas de Atlassian.
- Revisar access logs buscando traversal codificado o doblemente codificado.
- Priorizar instancias públicas y revisar archivos sensibles.

FILE SERVER / RCE

Rejetto HFS: falsificación de sesión administrativa lleva a RCE

REJETTO HFS CVE-2026-61500 RCE



QUÉ ESTÁ PASANDO

Se reportó explotación activa de CVE-2026-61500. HFS 3.0.0–3.2.0 usa `Math.random()` para generar la clave de firma de sesión; un atacante puede reconstruirla, falsificar una sesión administrativa y usar `server_code` para ejecutar comandos.

POR QUÉ IMPORTA

Un HFS publicado en Internet puede pasar de intercambio de archivos a punto de entrada con privilegios administrativos. La explotación comenzó a observarse alrededor del 1 de Octubre y ya existe código de explotación público.

QUÉ REVISAR AHORA

- Identificar HFS 3.0.0–3.2.0 y actualizar a una versión corregida.
- Revisar ráfagas de solicitudes de login y sesiones administrativas.
- Auditar cambios en `server_code`.
- Revisar archivos nuevos y conexiones salientes.

Cisco: ola de vulnerabilidades críticas en infraestructura de red

NX-OS APIC SSM ON-PREM MERAKI



QUÉ ESTÁ PASANDO

Cisco publicó una ola de avisos para NX-OS, APIC, License/SSM On-Prem y Meraki. Incluye RCE no autenticadas de CVSS 9.8 en NX-OS y APIC, y una falla de CVSS 10.0 en SSM On-Prem. El NX-API (CVE-2026-76471) permite RCE como root cuando está habilitado.

Cisco indicó que estas fallas fueron identificadas en revisiones internas y no eran conocidas como explotadas al publicar los avisos.

POR QUÉ IMPORTA

El riesgo está en la concentración de privilegios: estas plataformas administran red, data center y licenciamiento. Un compromiso podría afectar configuración, disponibilidad y credenciales de múltiples sistemas.

La prioridad es identificar exposición y corregir; no debe confundirse con una campaña de explotación activa.

QUÉ REVISAR AHORA

- Inventariar NX-OS, APIC, SSM On-Prem y Meraki afectados.
- Confirmar si NX-API u otras interfaces administrativas están habilitadas.
- Aplicar las versiones corregidas de Cisco.
- Revisar cambios administrativos anómalos y accesos desde redes no autorizadas.

DEVOPS / OBSERVABILIDAD

GitLab y Splunk: nuevas fallas críticas en plataformas centrales

GITLAB SPLUNK CI/CD REST API



QUÉ ESTÁ PASANDO

GitLab publicó el CVE-2026-97229, CVSS 10.0, una RCE en el compilador de expresiones de CI/CD. El 7 de Octubre Splunk publicó 17 vulnerabilidades en Enterprise; CVE-2026-76268 alcanza CVSS 9.8 y permite a un usuario no autenticado con acceso de red al Patroni REST API ejecutar comandos en un Search Head Cluster.

POR QUÉ IMPORTA

GitLab concentra código, secretos, runners y credenciales de despliegue. Splunk concentra telemetría y funciones de búsqueda; comprometer cualquiera de las dos plataformas puede abrir acceso a información sensible o capacidades útiles para ataques posteriores.

QUÉ REVISAR AHORA

- Identificar GitLab self-managed y Splunk Enterprise afectados.
- Actualizar a las versiones corregidas.
- GitLab: revisar pipelines, runners, usuarios y tokens.
- Splunk: restringir Patroni REST API y revisar actividad administrativa.

CREDENCIALES / RANSOMWARE

FortiBleed: credenciales comprometidas siguen alimentando accesos ransomware

FORTIBLEED FORTIGATE SSL VPN

**QUÉ ESTÁ PASANDO**

El FBI y USSS actualizaron la campaña FortiBleed: credenciales comprometidas se reutilizan contra FortiGate y SSL VPN mediante credential stuffing y password spraying. Inteligencia reciente sobre TheGentlemen describe además el uso de BYOVD para detener AV/EDR antes del despliegue de ransomware.

POR QUÉ IMPORTA

El riesgo no termina en el FortiGate. Una cuenta válida puede convertirse en acceso inicial y después en persistencia y evasión en endpoints. La cadena conecta robo de credenciales, acceso remoto y ransomware.

QUÉ REVISAR AHORA

- Auditar cuentas locales y administrativas de FortiGate.
- Buscar lockouts, password spraying y accesos VPN anómalos.
- Revisar drivers sospechosos y señales de AV/EDR deshabilitado.
- Correlacionar IOCs del advisory JCSA-20261006-01 con actividad posterior.

APT / INFRAESTRUCTURA CRÍTICA

Flax Typhoon: infraestructura de escaneo y spearphishing desmantelada

FLAX TYPHOON MICROSCAN FISHHUB



QUÉ ESTÁ PASANDO

FBI/DOJ y socios internacionales anunciaron el desmantelamiento de infraestructura vinculada a Integrity Technology Group y actividad consistente con Flax Typhoon. MicroScan y FishHub se usaban para escanear y apoyar intrusiones y spearphishing.

POR QUÉ IMPORTA

El caso muestra una operación a escala: reconocimiento automatizado, explotación de servicios vulnerables, password spraying contra correo y persistencia mediante herramientas legítimas. La disrupción de dominios no elimina necesariamente toda la capacidad operativa.

QUÉ REVISAR AHORA

- Revisar exposición externa y servicios legacy.
- Correlacionar password spraying contra M365/Exchange y VPN.
- Buscar SoftEther renombrado como conhost.exe o dllhost.exe.
- Revisar los dominios e infraestructura publicados en AA26-281A.

Supply chain: firmware móvil y software de IA amplían la superficie

MIDNIGHT MIMOSA TENSORLAKE LANGFLOW



QUÉ ESTÁ PASANDO

Midnight Mimosa llega preinstalado en firmware de ciertos Android económicos MediaTek; Bitdefender observó presencia en más de 150 países, incluido México. En software, tensorlake@0.5.144 fue publicado el 8 de Octubre con una variante de Shai-Hulud que roba secretos durante npm install. IBM también publicó varias fallas críticas de Langflow, incluida CVE-2026-93674 (CVSS 9.8).

POR QUÉ IMPORTA

Son tres riesgos de cadena de suministro en puntos distintos: un teléfono puede llegar comprometido desde fábrica; un paquete legítimo puede comprometer al desarrollador o CI/CD; y una plataforma de agentes puede exponer ejecución de código y secretos del entorno.

QUÉ REVISAR AHORA

- Android: validar firmware, procedencia y dispositivos con MFA/VPN/correo.
- Tensorlake: buscar 0.5.144 en lockfiles, caches y runners.
- Si hubo 0.5.144, aislar y rotar secretos tras retirar persistencia.
- Langflow: identificar versiones 1.0.0–1.12.2 y actualizar a 1.12.3.

RANSOMWARE / EXTORSIÓN

Ransomware: nuevos claims en México/LATAM y presión de TheGentlemen

QILIN THEGENTLEMEN LATAM CLAIMS



QUÉ ESTÁ PASANDO

Se identificaron claims contra MCM Telecom, Grupo Industrial Tauro y Ladrillera Mecanizada en México; en LATAM, contra organizaciones de Brasil, Colombia y Argentina. TheGentlemen añadió **Deloitte** el 9 de Octubre y **Confluent** el 12 de Octubre.

Los monitores regionales mantienen estos casos como alegaciones; el listado no demuestra por sí solo intrusión, exfiltración o cifrado.

POR QUÉ IMPORTA

La señal útil para CTI es buscar exposición antes de que el claim se convierta en incidente: credenciales comprometidas, accesos VPN/RDP, abuso de herramientas legítimas y muestras de datos. Deloitte y Confluent elevan el interés por el tipo de información que podrían manejar, pero no debe asumirse compromiso.

QUÉ REVISAR AHORA

- Validar si la organización aparece en los listados y desde qué fecha.
- Buscar credenciales expuestas, VPN/RDP y cuentas nuevas.
- Monitorear muestras, volúmenes o evidencia técnica publicada.
- Mantener cada caso como claim hasta obtener corroboración independiente.

BraZetsu: toolkit de Initial Access Brokers dirigido a LATAM

BRAZETSU EXILWARE LATAM



QUÉ ESTÁ PASANDO

El valor de la amenaza está en el acceso que genera: un endpoint comprometido puede terminar vendido a otro actor para fraude, robo de información o ransomware. Group-IB identificó versiones dirigidas a plataformas de comercio electrónico y servicios financieros de Brasil, Argentina, México y Chile.

POR QUÉ IMPORTA

BraZetsu puede ser el primer eslabón de una intrusión que posteriormente cambia de manos. Para organizaciones de LATAM, el riesgo aumenta cuando equipos con acceso a VPN, RDP, certificados o aplicaciones financieras son comprometidos.

QUÉ REVISAR AHORA

- Buscar Python no autorizado y ejecución de cmd.exe desde endpoints.
- Revisar acceso a certificados PFX/P12, OneDrive y recursos compartidos.
- Buscar enumeración anómala de procesos, aplicaciones y servicios.
- Correlacionar infect[.]online y c2[.]installcenter[.]com con telemetría.

Operation KillSwitch: desmantelamiento de KillSec

KILLSEC KILLSWITCH RANSOMWARE



QUÉ ESTÁ PASANDO

Europol confirmó el 1 de Octubre Operation KillSwitch contra KillSec: tres arrestos, ocho registros y control de sus servidores y leak site. Las autoridades aseguraron al menos 110 TB y vinculan la operación con alrededor de 1,000 ataques.

POR QUÉ IMPORTA

Es una disrupción confirmada de una operación RaaS con actividad internacional y presencia documentada en LATAM. También permite revisar retrospectivamente si la organización fue publicada por KillSec o quedó expuesta en campañas anteriores.

QUÉ REVISAR AHORA

- Revisar si la organización apareció históricamente en KillSec.
- Correlacionar incidentes anteriores con IOCs conocidos.
- Revisar RDP, aplicaciones expuestas y credenciales comprometidas.
- Validar terceros con acceso a información sensible.

Indicadores y hunting – AhsayCBS, SonicWall y HFS



AHSAYCBS

- imagefiles-backup.oss-ap-southeast-7.aliyuncs[.]com
- xmr.kryptex[.]network:8029
- 51.195.127[.]124:8029
- **SHA256 msedge.exe:**
05f69ae6b2b89c1c4dcf836bff032232f11bf0109f2b498e2345045d06139034
- **SHA256 edge.exe:**
4dcb0202fe8b2d4d7b183764e38184cd6ed50132786cc7e7d1f7f4bce1dd6f3d
- **SHA256 Taskgmr.ps1:**
481728a7c9c4c02be07051d9c1958d902ea6397ebb8952ab83944818e3d25d21

SMA1000 / HFS

- **SMA1000:** revisar solicitudes *WorkPlace* y actividad administrativa.
- **HFS:** revisar sesiones forjadas, ráfagas de login y cambios en *server_code*.

Indicadores y hunting – FortiBleed y Flax Typhoon



FORTIBLEED

- Cuentas observadas:
 - forticloud-sync
 - support_Fortinet
 - adminsslvpn
- Buscar cuentas locales nuevas, lockouts y password spraying.
- Revisar IPs del advisory *FBI/USSS JCSA-20261006-01*.

FLAX TYPHOON / AA26-281A

- 98aiblog[.]com
- hmbcloud[.]com
- hmbcloud[.]net
- hmbiplc-01[.]com
- javacheck[.]ooguy[.]com
- javaupdate[.]giize[.]com
- sexytube0[.]com
- twimg[.]co[.]uk
- Buscar SoftEther renombrado y password spraying contra *Exchange/M365*.

Indicadores y hunting – Midnight Mimosa y Tensorlake

ANDROID TENSORLAKE SHAI-HULUD



MIDNIGHT MIMOSA

- `api.weatherlive[.]world/br_upgrade/upgradeV2/getConfigs`
- `api.weatherlive[.]world/odborwer_dot/cm`
- `oss.showtimetool[.]com`
- `85.17.70.38:6000 · 39.96.8.180:9008 · 120.78.215.151:80`
- `com.android.system.lite · com.mobile.applock.en/.wt/.tg`

TENSORLAKE / SHAI-HULUD

- `tensorlake@0.5.144`
- `iseekaigogo[.]com`
- **SHA256 setup.mjs:**
`25a0735d0db7dc40e5d45ce42d9c106067e6a66e184d967cfecfab17c3bcb5ef`
- **SHA256 Math_Symbol.js:**
`b50a00900399ba99fb6ce1fc151519cb99d44320ef2a631f2237e1aea0ad6fec`

LO MÁS RELEVANTE DEL CORTE

La exposición a Internet y la cadena de suministro concentran el riesgo



- **AhsayCBS**: RCE explotada con webshells y cryptomining en backup.
- **SonicWall SMA1000**: CVSS 10 y señales de explotación.
- **Cisco**: ola de RCE críticas en NX-OS, APIC y SSM On-Prem.
- **FortiBleed**: credenciales reutilizadas como acceso inicial para ransomware.
- **GitLab/Splunk**: nuevas fallas críticas en CI/CD y observabilidad.
- **Tensorlake**: paquete npm legítimo comprometido con Shai-Hulud.
- **Midnight Mimosa**: firmware Android comprometido con presencia en México.
- **Flax Typhoon**: infraestructura de reconocimiento y spearphishing intervenida.

OBSERVACIÓN / MÉXICO

Ransomware en México: seguimiento sin sobreatribuir

MÉXICO CLAIMS HUNTING



- ❑ **MCM Telecom** | Qilin – 8 de Octubre
- ❑ **Grupo Industrial Tauro** | Lamashtu – 5 de Octubre
- ❑ **Ladrillera Mecanizada** | ArcusMedia – 9 de Octubre

Ransomware.mx mantiene los tres como publicaciones sin corroboración independiente. La fecha corresponde al claim observado, no necesariamente al momento del acceso.

Revisar: credenciales expuestas, VPN/RDP, cuentas nuevas, actividad de exfiltración y cualquier IOC publicado posteriormente.

OBSERVACIÓN / LATAM

LATAM: nuevos claims y expansión regional de Qilin

LATAM QILIN NIGHTSPIRE UMBRA



- ❑ **INI Fiocruz** | NightSpire – 8 de Octubre, Brasil
- ❑ **SOCOCO** | UmBra – 8 de Octubre, Brasil
- ❑ **Dipecarr** | Eclipse – 8 de Octubre, Brasil
- ❑ **Petrosul** | DragonForce – 7 de Octubre, Brasil
- ❑ **Confipetrol** | Qilin – 11 de Octubre, Colombia
- ❑ **Secretaría de Modernización e Innovación** – 10 de Octubre, Argentina

No existe evidencia pública suficiente para afirmar intrusión, cifrado o exfiltración. Las fechas corresponden a publicaciones observadas.



RADAR CTI

BOLETÍN SEMANAL DE CIBERSEGURIDAD

Las amenazas cambian
cada semana.

Tu capacidad de responder
define el impacto.



¿Tu organización podría
detectar alguno de estos
escenarios antes de que
afecte la operación?

En Grupo Smartekh ayudamos a
equipos de TI y ciberseguridad a:

- Identificar riesgos críticos
- Priorizar vulnerabilidades
- Fortalecer controles
- Responder incidentes con rapidez real



NEXT GEN SOC
Monitoreo 24/7



THREAT INTELLIGENCE
Inteligencia accionable



**VULNERABILITY
MANAGEMENT**
Visibilidad y remediación



ESCRÍBENOS
informacion@smartekh.com

#SMARTEKH



Canal
WhatsApp



Eventos



Blogs



Infografías
Awareness

