GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °2526

BOLETÍN DE CIBERSEGURIDAD SEMANAL

Bienvenido a su boletín semanal de ciberseguridad generado por Gamma Ingenieros. A través de esta publicación tenemos el propósito de compartir contenidos relevantes para nuestras operaciones y aliados de negocio.

Aquí encontrará información sobre vulnerabilidades, alertas tempranas, noticias del sector, incidentes de ciberseguridad, tecnologías y servicios relacionados, entre otros.

VISTA RÁPIDA

	CRÍTICO	URGENTE	IMPORTANTE
VULNERABILIDADES	2	1	0
MALWARE	0	1	0
NOTICIAS DE CIBERSEGURIDAD	0	1	0

VULNERABILIDADES

CVE-2026-42530 Y CVE-2026-42055 – F5 NGINX (EJECUCIÓN REMOTA DE CÓDIGO Y DENEGACIÓN DE SERVICIO)

Se han divulgado dos vulnerabilidades críticas fuera de banda que afectan a NGINX Open Source, NGINX Plus y productos derivados. Estos fallos permiten a atacantes remotos no autenticados provocar la caída continua de los procesos de trabajo (Denegación de Servicio) o potencialmente ejecutar código arbitrario en los sistemas afectados bajo configuraciones específicas de procesamiento de protocolos web modernos.

Resumen técnico:

- Identificador principal: CVE-2026-42530 y CVE-2026-42055 (ID de desarrollo de F5: NPS-8).
- Severidad: Crítica (Puntaje base de 9.2 en CVSS v4.0).
- Causa raíz: Un error de uso después de liberar (Use-After-Free) en el módulo ngx_http_v3_module originado por un desajuste en el tiempo de vida de los punteros (lifetime mismatch), y un desbordamiento de búfer basado en memoria dinámica (Heap-based Buffer Overflow) en los módulos ngx_http_proxy_v2_module y ngx_http_grpc_module por una anomalía de diseño en el codificador varint de HPACK.
- Mecanismo de falla: Para CVE-2026-42530, el atacante reabre un flujo de codificador QPACK mediante una sesión HTTP/3 maliciosa, dejando un puntero a nivel de sesión apuntando a memoria de un flujo que ya fue cerrado y liberado. Para CVE-2026-42055, el fallo se activa al intermediar tráfico HTTP/2 o gRPC (usando proxy_http_version 2 o grpc_pass), manteniendo la directiva ignore_invalid_headers en off y un tamaño de large_client_header_buffers superior a 2 MB, lo que causa que peticiones sobredimensionadas escriban datos controlados por el atacante en regiones de memoria no autorizadas.
- Estado de explotación: No se registran ataques activos en el entorno real ni exploits públicos disponibles al momento de su divulgación oficial a mediados de junio de 2026. No obstante, incidentes previos muy recientes en este tipo de componentes (como el denominado NGINX Rift / CVE-2026-42945) sufrieron explotación masiva en la naturaleza a los pocos días de su publicación, elevando la urgencia preventiva.
- Versiones afectadas: NGINX Open Source 1.31.0 a 1.31.1 (CVE-2026-42530) y 1.30.0 a 1.30.2 / 1.31.1 (CVE-2026-42055); NGINX Plus ramas R33 a R36 y versiones 37.0.0 a 37.0.1; así como componentes integrados de NGINX Gateway Fabric, Instance Manager e Ingress Controller en sus ramas activas.

Impacto potencial:

- Ejecución remota de código arbitrario (RCE): Si el mecanismo de protección ASLR (Address Space Layout Randomization) está desactivado en el sistema operativo subyacente o si el atacante logra eludirlo empleando técnicas complementarias, la corrupción de memoria concede la capacidad de ejecutar comandos arbitrarios con los privilegios del proceso de NGINX.
- Denegación de servicio (DoS) sostenida en la infraestructura: El envío automatizado de solicitudes malformadas o sobredimensionadas provoca el colapso y reinicio recurrente de los procesos de trabajo (worker processes), interrumpiendo por completo la disponibilidad de las aplicaciones y servicios web legítimos expuestos a internet.
- Compromiso total del ecosistema de microservicios: Al impactar directamente sobre componentes de orquestación crítica como NGINX Ingress Controller y NGINX Gateway Fabric, una intrusión exitosa otorga al atacante visibilidad, interceptación y control potencial sobre todo el tráfico entrante a un clúster de Kubernetes.
- Punto de entrada perimetral para movimiento lateral profundo: Vulnerar el balanceador de carga o proxy inverso principal sitúa a los actores de amenazas en una posición privilegiada dentro de la DMZ para realizar escaneos internos hacia zonas sensibles de la red corporativa o atacar servidores de gestión de identidades.

Recomendaciones de mitigación:

1. Actualización inmediata a las versiones seguras de soporte: Se urge a los administradores a migrar con prioridad los despliegues de la organización hacia las versiones oficiales corregidas por el fabricante: NGINX Open Source 1.31.2 (mainline) o 1.30.3 (stable), NGINX Plus 37.0.2.1 o R36 P6, y NGINX Gateway Fabric 2.6.4.
2. Desactivación temporal del protocolo HTTP/3: Si no es posible aplicar parches de inmediato, eliminar la instrucción quic de las directivas listen para desactivar HTTP/3 QUIC y mitigar la CVE-2026-42530 (Use-After-Free).
3. Ajuste y endurecimiento de cabeceras HTTP/2 (Mitigación CVE-2026-42055): Modificar las configuraciones de los proxies e interfaces NGINX eliminando explícitamente la instrucción ignore_invalid_headers off (para restablecer el valor predeterminado on que valida los headers) y asegurar que el tamaño asignado a large_client_header_buffers se reduzca estrictamente por debajo de los 2 MB.

4. Auditoría forense preventiva y monitoreo de logs: Realizar un inventario exhaustivo de cada balanceador expuesto a internet y configurar alertas en la solución SIEM centralizada orientadas a trazar caídas o reinicios anómalos de los procesos trabajadores (worker crashes), monitorizando volumetrías inusuales en conexiones gRPC o proxies HTTP/2.

Prioridad: Crítica.

Ampliar información:

- https://cybersecurefox.com/en/f5-critical-nginx-vulnerabilities-cve-2026-42530-42055/
- https://my.f5.com/manage/s/article/K000161616
- https://socprime.com/es/blog/cve-2026-42530-fallo-critico-nginx-http-3-puede-desencadenar-dos-y-posible-rce/
- https://thehackernews.com/2026/06/f5-patches-two-critical-nginx-open.html
- https://csirt.telconet.net/comunicacion/boletines-servicios/advertencia-critica-sobre-vulnerabilidades-en-nginx-con-riesgo-de-ejecucion-de-codigo-arbitrario-y-ataques-dos/

CVE-2026-47729 – SQUID PROXY (FUGA DE INFORMACIÓN EN MEMORIA - "SQUIDBLEED")

Se descubrió una vulnerabilidad histórica de divulgación de información en Squid, originada en código heredado de enero de 1997. Denominada "Squidbleed", permite extraer memoria dinámica (heap) que contienen solicitudes HTTP en texto plano de otros usuarios legítimos, exponiendo credenciales de acceso y tokens de sesión activos.

Resumen técnico:

- Identificador principal: CVE-2026-47729 (Alias: Squidbleed/TA2026175).
- Severidad: Crítica (Puntaje base de 9.1 en CVSS v3.0).
- Causa raíz: Una falla de lectura fuera de límites en el búfer de la memoria dinámica (Heap Over-read / CWE-125) dentro del analizador sintáctico de listados de directorios FTP (FTP directory listing parser), combinada con el reciclaje de búferes de memoria de 4KB (MEM_4K_BUF) por parte de Squid sin realizar un borrado completo o inicialización a cero (without zeroing them).
- **Mecanismo de falla:** El error reside en una lógica de **1997** diseñada para compatibilidad con servidores FTP antiguos de **NetWare**. Al procesar espacios en blanco mediante un bucle basado en **strchr**, un servidor FTP malicioso puede responder con una línea que termina tras la marca de tiempo (sin nombre de archivo), dejando el puntero sobre el terminador nulo (**\0**). Como el estándar de **C** considera el byte nulo parte de la búsqueda, **strchr** devuelve un puntero válido y el bucle continúa indefinidamente, supera el límite del búfer y copia con **xstrdup** memoria adyacente del **heap**, enviándola al atacante como nombre de archivo. Al reutilizarse búferes de peticiones **HTTP**, se filtran datos residuales de otros usuarios en la respuesta del listado FTP.
- Estado de explotación: No se registra explotación activa en entornos reales al momento de su divulgación masiva a finales de junio de 2026, sin embargo, el código de prueba de concepto (PoC) ya ha sido publicado en repositorios abiertos de GitHub, lo que eleva significativamente el riesgo. El fallo fue descubierto de forma automatizada mediante auditoría de código asistida por inteligencia artificial (modelo Claude Mythos Preview).
- Versiones afectadas: Todas las versiones activas de Squid en su configuración por defecto anteriores al parche oficial. El mantenimiento del software integró la corrección definitiva en la versión Squid 7.7.

Impacto potencial:

- Fuga masiva de credenciales y tokens de autenticación: La sobrelectura de los búferes de memoria compartidos expone directamente cabeceras sensibles de peticiones HTTP en texto plano, tales como Authorization, tokens de tipo Bearer o cookies de sesión corporativas de otros usuarios de la red.
- Secuestro de sesión y suplantación de identidad (Session Hijacking): Un atacante que extraiga exitosamente cabeceras de autorización de una víctima puede reutilizar de inmediato los tokens interceptados para autenticarse y suplantar al usuario comprometido en los servicios y aplicaciones web de destino sin levantar sospechas.
- Compromiso de tráfico interceptado bajo inspección SSL/TLS: En aquellas infraestructuras corporativas donde Squid está configurado como un proxy de interceptación y descifrado de tráfico TLS (inspección HTTPS), el contenido que usualmente viaja cifrado se vuelve legible en texto plano en los búferes del proceso, haciéndolo vulnerable a esta filtración de memoria.
- Espionaje interno en arquitecturas de redes compartidas: Dado que el ataque se cataloga como una amenaza interna o proveniente de un "cliente de confianza" (alguien con autorización de salida a través del proxy), un actor malicioso o un dispositivo comprometido dentro de redes corporativas, instituciones educativas o redes Wi-Fi públicas puede explotar de manera continua el fallo para espiar los datos de navegación de su entorno.

Recomendaciones de mitigación:

1. Desactivación absoluta del protocolo FTP en el proxy: Se recomienda como la medida inmediata más eficaz deshabilitar por completo el procesamiento de tráfico FTP en Squid. Debido a que los navegadores modernos basados en Chromium retiraron el soporte de FTP de forma nativa, el uso legítimo de este protocolo es casi nulo en redes corporativas actuales; remover el puerto 21 de la lista de puertos seguros (Safe_ports) y bloquearlo perimetralmente remueve por completo la superficie de ataque sin requerir un reinicio complejo.

2. Actualización del componente y verificación manual del parche: Actualizar las instancias de Squid a la versión oficial 7.7. Debido a inconsistencias iniciales en los reportes de las ramas de lanzamiento, es mandatorio que el equipo técnico valide directamente en el código fuente (archivo src/clients/FtpGateway.cc) la presencia del control de seguridad implementado: while (*copyFrom && strchr(w_space, *copyFrom)).

3. Rotación obligatoria de secretos transmitidos en texto plano: En organizaciones que confirmen el despliegue de versiones vulnerables de Squid, se debe realizar una auditoría de accesos y forzar la rotación inmediata de contraseñas, tokens de API y llaves de acceso de aquellos servicios internos o aplicaciones externas que hayan operado sobre HTTP sin cifrar durante el periodo de exposición.

4. Migración estructural hacia esquemas de cifrado de extremo a extremo: Forzar de manera estricta que todas las aplicaciones e integraciones internas utilicen protocolos criptográficos HTTPS nativos. El tráfico HTTPS estándar transmitido mediante el comando CONNECT viaja de forma opaca como un túnel para el proxy, impidiendo que sus cabeceras sean depositadas en los búferes reutilizables expuestos por el fallo.

Prioridad: Urgente.

Ampliar información:

- https://blog.calif.io/p/squidbleed-cve-2026-47729
- https://thehackernews.com/2026/06/29-year-old-squid-proxy-bug-squidbleed.html
- https://www.iansresearch.com/resources/all-blogs/post/security-blog/2026/06/24/researchers-uncover--squidbleed---29-year-old-squid-proxy-flaw
- https://www.hivepro.com/threat-advisory/squidbleed-decades-old-parser-flaw-exposes-sensitive-proxy-data
- https://blog.segu-info.com.ar/2026/06/squidbleed-cve-2026-47729-expone.html
- https://www.it-connect.tech/squidbleed-29-year-old-squid-proxy-flaw-leaks-user-credentials/

CVE-2026-20230 – CISCO UNIFIED COMMUNICATIONS MANAGER (FORJADO DE SOLICITUDES EN EL LADO DEL SERVIDOR Y ESCRITURA DE ARCHIVOS CON ELEVACIÓN A ROOT)

Se ha detectado la explotación activa en entornos reales de una vulnerabilidad crítica que afecta al componente de gestión de telefonía IP empresarial Cisco Unified Communications Manager (Unified CM). El fallo permite a atacantes remotos no autenticados realizar ataques de falsificación de solicitudes del lado del servidor (SSRF), escribir archivos arbitrarios dentro del sistema operativo subyacente y lograr la escalada completa de privilegios hasta el nivel de superusuario (root).

Resumen técnico:

- Identificador principal: CVE-2026-20230
- Severidad: Alta / Crítica (Puntaje base de 8.6 en CVSS).
- Causa raíz: Una validación de entrada deficiente al procesar solicitudes HTTP específicas dirigidas al componente WebDialer.
- Mecanismo de falla: El atacante envía una petición HTTP maliciosa con URI file:// para abusar de WebDialer y escribir archivos con contenido controlado en rutas estratégicas del sistema, evadiendo la autenticación. Las campañas despliegan servicios falsificados de Apache Axis para inyectar un cargador de archivos JSP que deposita una webshell de ejecución de comandos en /platform-services/axis2-web/.
- Estado de explotación: Explotación activa confirmada en la naturaleza. Firmas de inteligencia de amenazas detectaron barridos automatizados y ataques exitosos procedentes de la red Tor durante el penúltimo fin de semana de junio de 2026. La publicación de los detalles técnicos y del código de prueba de concepto (PoC) público por parte de equipos de divulgación de vulnerabilidades ha acelerado los intentos de explotación masiva.
- Versiones afectadas: Cisco Unified Communications Manager (Unified CM) y Cisco Unified Communications Manager Session Management Edition (Unified CM SME) en versiones previas a los parches oficiales. El fallo requiere de forma mandatoria que el servicio opcional WebDialer se encuentre habilitado (el cual viene desactivado por defecto).

Impacto potencial:

- Escalada de privilegios a Root: Al utilizar la primitiva de escritura arbitraria de archivos, un actor de amenazas puede sobrescribir configuraciones del sistema, scripts de inicio o tareas cron para ejecutar comandos con los máximos privilegios posibles (root), otorgándole el control total del servidor subyacente.
- Ejecución remota de código (RCE) persistente: La inyección exitosa de webshells en los directorios de servicios web de la plataforma expone una interfaz de acceso continuo para que el atacante administre comandos remotamente sin interactuar con los canales legítimos de gestión.
- Interrupción y espionaje de comunicaciones corporativas: Al comprometer la infraestructura central de telefonía IP y control de llamadas de la organización, el atacante se posiciona para manipular el enrutamiento de voz, monitorizar flujos de datos sensibles, acceder a registros de llamadas corporativas o comprometer servicios de mensajería unificada.
- Pivoteo hacia redes de confianza interna: Los servidores Unified CM se encuentran profundamente integrados en el tejido de confianza de la infraestructura de red empresarial (conectados a bases de datos, directorios activos y servidores de red interna), convirtiendo al dispositivo comprometido en un punto de origen ideal para movimientos laterales profundos.

Recomendaciones de mitigación:

1. Deshabilitación inmediata del servicio WebDialer: Como contramedida de mitigación temporal y de impacto inmediato si no es posible programar un parcheo de emergencia, se debe proceder a detener y desactivar el servicio afectado. Esto se realiza desde la interfaz de administración de Cisco Unified Serviceability -> Tools -> Control Center - Feature Services -> Sección CTI Services, cambiando el estado de Cisco WebDialer Web Service a "Not Running".

2. Aplicación inmediata de actualizaciones del fabricante: Actualizar de manera prioritaria el software de los appliances Unified CM a las versiones oficiales que contienen la solución definitiva: rama 14 a la versión 14SU6 y rama 15 hacia la versión 15SU5 (o aplicar los parches COP recomendados por el soporte de Cisco).
3. Búsqueda activa de Indicadores de Compromiso (Threathunting): Auditar los sistemas de archivos de los servidores de comunicaciones en busca de anomalías de creación de archivos recientes, particularmente inspeccionando rutas bajo /tmp/ (como el archivo de prueba detectado en escaneos iniciales cve-2026-20230-test.txt) y buscando scripts .jsp sospechosos dentro de los directorios de servicios de /platform-services/axis2-web/.
4. Segmentación de red y restricción de interfaces: Asegurar que las interfaces de administración web y los servicios de Unified CM orientados a red no se encuentren expuestos directamente a internet. Aplicar listas de control de acceso (ACL) estrictas y firewalls perimetrales para permitir tráfico únicamente desde segmentos de red de administración aislados y redes internas estrictamente necesarias.

Prioridad: Crítica.

Ampliar información:

- https://unaaldia.hispasec.com/explotan-en-ataques-un-fallo-critico-en-cisco-nified-cm-con-webdialer-habilitado/
- https://thehackernews.com/2026/06/cisco-unified-cm-flaw-exploited-after.html
- https://www.linkedin.com/pulse/cisco-unified-cm-vulnerability-actively-exploited-guh8e
- https://www.helpnetsecurity.com/2026/06/24/cisco-unified-cm-flaw-exploited-to-drop-webshells-cve-2026-20230/
- https://www.theregister.com/security/2026/06/24/the-hits-keep-on-coming-for-cisco-vulnerabilities/5261797
- https://www.securityweek.com/hackers-exploiting-cisco-unified-cm-vulnerability/

MALWARE

FRAMEWORK GENTLEKILLER – SUITE DE EVASIÓN Y DESACTIVACIÓN DE EDR (ASOCIADO A GENTLEMEN RANSOMWARE)

Se han revelado los análisis detallados sobre "GentleKiller", un framework interno de desactivación de herramientas de seguridad (EDR Killer) desarrollado y mantenido de forma centralizada por la organización criminal de Ransomware-as-a-Service (RaaS) conocida como "Gentlemen". A diferencia de otros grupos que delegan la desactivación de defensas en sus afiliados, los operadores de Gentlemen proveen esta suite completamente estructurada para cegar las soluciones Antivirus y EDR de las víctimas antes de proceder con el despliegue del payload de cifrado.

Resumen técnico:

- Tipo de amenaza: Framework de evasión de defensas y desactivación de soluciones de seguridad (EDR/AV Killer) mediante técnicas BYOVD (Bring Your Own Vulnerable Driver).
- Alias: GentleKiller, GentleKiller Suite.
- Desarrollador / Grupo asociado: Banda RaaS Gentlemen (operada bajo el liderazgo del actor de amenazas conocido como hastalamuerte o zeta88).
- Mecanismo de acción: El framework opera mediante al menos ocho variantes distintas, cada una diseñada para instalar y abusar de un controlador de kernel (driver) específico de un tercero legítimo pero vulnerable, o bien mediante rootkits personalizados (ej. eb.sys de Kaspersky, nseckrnl.sys de FACEIT Anti-Cheat, GameDriverX64.sys de Valorant, los controladores stpm_old.sys y stpm_new.sys de Safetica, dmx.sys de Zemana, 360netmon_wfp.sys de Qihoo 360, IMFForceDelete de IObit, y el rootkit PoisonX). Utiliza llamadas nativas de Windows y comandos IOCTL (Input/Output Control) en el espacio de kernel (Anillo 0 / Ring 0) para forzar de manera recurrente la terminación de los procesos de seguridad. Adicionalmente, integran herramientas externas estandarizadas como HexKiller, ThrottleBlood y HavocKiller.

- Estrategia de evasión: Aplica protección binaria avanzada post-compilación utilizando empaquetadores como Enigma o Themida. Los archivos ejecutables se renombran y configuran para suplantar la identidad de proveedores tecnológicos legítimos de ciberseguridad, inyectando información de versión falsificada, iconos clonados y firmas digitales inválidas copiadas de binarios originales.
- Objetivos / Procesos atacados: Monitorea y finaliza sistemáticamente en un bucle cerrado más de 400 procesos pertenecientes a 48 productos de seguridad y supervisión de endpoints globales (incluyendo soluciones críticas de CrowdStrike, SentinelOne, Microsoft Defender, Sophos, Carbon Black, ESET, Sysmon, entre otros).

Impacto potencial:

- Inhabilitación total de alertas y telemetría de seguridad (EDR/AV): Al bloquear y finalizar de manera forzada los agentes de protección local, los equipos de defensa y los centros de operaciones de seguridad (SOC) pierden visibilidad absoluta de las actividades sospechosas que ocurren dentro del endpoint comprometido.
- Cifrado desatendido de activos críticos: La remoción de las barreras de protección de endpoint facilita que los afiliados desplieguen sin interferencias los cifradores de la banda, los cuales incluyen variantes en Go para plataformas Windows y Linux, así como ejecutables optimizados en C dirigidos a hipervisores VMware ESXi.
- Robo masivo y exfiltración de credenciales corporativas: El uso de esta suite se ha vinculado operativamente con el despliegue de herramientas complementarias como OxideHarvest (un credential stealer escrito en Rust), diseñado para extraer contraseñas, cookies y datos de sesiones de más de una decena de navegadores web basados en Chromium y Gecko.
- Persistencia evasiva a nivel de Kernel: Al explotar vulnerabilidades en controladores firmados digitalmente (BYOVD), los atacantes manipulan directamente la memoria del sistema operativo a nivel de kernel, impidiendo que herramientas de seguridad tradicionales de nivel de usuario (user-mode) puedan interceptar, auditar o mitigar la intrusión.

Recomendaciones de mitigación:

1. Implementación estricta de políticas de control de controladores: Configurar y hacer cumplir directivas de integridad de código y control de aplicaciones (como WDAC o HVCI en entornos Windows) utilizando listas de bloqueo actualizadas (como la Microsoft Vulnerable Driver Blocklist) para impedir de forma mandatoria la carga de controladores de kernel conocidos por ser susceptibles a explotación BYOVD.
2. Auditoría forense de servicios y telemetría DeviceIoControl: Monitorea mediante herramientas de registro de eventos (como Windows Sysmon) la creación inusual de servicios del sistema asociados a drivers de terceros no autorizados y audita patrones inusuales de comunicación a través de APIs nativas dirigidas a interactuar con controladores en modo kernel.
3. Restricción rigurosa de privilegios administrativos locales: Debido a que la técnica BYOVD requiere obligatoriamente que el atacante posea privilegios de administrador local para instalar y arrancar el servicio del driver malicioso/vulnerable, se debe aplicar de forma estricta el principio de mínimo privilegio y robustecer los mecanismos de autenticación para mitigar accesos elevados no autorizados.
4. Monitoreo de bucles de terminación de procesos y rutas sospechosas: Configurar alertas específicas orientadas a detectar la presencia de directorios de almacenamiento temporales sospechosos (por ejemplo, carpetas nombradas como GentlemenCollection u homólogos) y vigilar la ejecución de comandos de consola o scripts que intenten invocar binarios empaquetados o con nombres simulados de agentes legítimos.

Prioridad: Urgente.

Ampliar información:

- https://www.welivesecurity.com/es/investigaciones/gentlekiller-analisis-del-framework-edr-killer-de-gentlemen/
- https://socprime.com/es/active-threats/matame-suavemente-dentro-del-marco-edr-killer-de-gentlemen/
- https://thehackernews.com/2026/06/the-gentlemen-raas-uses-gentlekiller.html
- https://securityaffairs.com/193941/malware/inside-gentlekiller-the-edr-killer-powering-the-gentlemen.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.

NOTICIAS DE CIBERSEGURIDAD

FORTIBLEED: COMPROMISO DE MÁS DE 430.000 DISPOSITIVOS FORTIGATE Y FILTRACIÓN INDUSTRIAL DE 110 MILLONES DE CREDENCIALES

Se ha revelado una expansión crítica de la operación global de ciberespionaje y robo de datos a gran escala conocida como "FortiBleed". Llevada a cabo por un intermediario de acceso inicial (IAB) de habla rusa motivado por el lucro, la campaña ha logrado comprometer más de 430.000 firewalls FortiGate en todo el mundo. A través del despliegue de analizadores de red personalizados y frameworks optimizados con Inteligencia Artificial, los atacantes han consolidado una base de datos histórica que supera los 110 millones de credenciales corporativas, afectando severamente el perímetro de organizaciones globales y pymes de servicios de TI.

Resumen técnico:

- Identificador principal: Campaña FortiBleed (Operación Global de Acceso Inicial Multivendedor).
- Severidad / Alcance: Alerta Máxima / Crítica. La campaña compromete aproximadamente al 50% de los firewalls Fortinet indexados y expuestos en el internet global, con un enfoque agresivo en pequeñas y medianas empresas (pymes) de menos de 200 empleados en regiones clave como Estados Unidos e India.
- Causa raíz e Higiene: Ataques masivos y automatizados de fuerza bruta, relleno de credenciales (credential stuffing) alimentados por fugas previas de infostealers, ausencia de doble factor de autenticación (MFA) y el abuso pasivo de comandos de diagnóstico integrados en el sistema operativo FortiOS.
- Mecanismo de ataque: La operación se ejecuta en ciclos estructurados de 300 minutos (5 horas) con 1.000 hilos simultáneos y restricciones de geolocalización vinculadas al horario comercial de Moscú (07:00 a 18:00). El flujo del compromiso se divide de forma estandarizada en 5 etapas operativas:

- Reconocimiento: Escaneo a gran escala mediante Masscan y Shodan; filtrado y segmentación geográfica de los objetivos con las utilidades FortiProbe-fast y GeoSplit.
- Compromiso: Ataques de diccionario y relleno de credenciales por SSH junto con el verificador "forticheck" enfocado en el panel administrativo y portales SSL-VPN para obtener accesos de nivel de administrador.
- Intercepción: Despliegue de la herramienta basada en Go FortigateSniffer, la cual ejecuta de manera encubierta el comando nativo de diagnóstico -diagnose sniffer packet de FortiOS para interceptar pasivamente el tráfico de autenticación de 24 protocolos en texto plano y hashes.
- Descifrado: Procesamiento masivo de hashes fuera de línea (offline) a través de las herramientas Hashmat y Hashtopolis, centralizadas y administradas mediante un bot de Telegram denominado HASHBOT.
- Exfiltración y Persistencia: Sustracción de datos confidenciales de recursos compartidos de red y uso de cookies de sesión robadas o cuentas duplicadas para mantener accesos persistentes legítimos.
- Estado de la campaña: Altamente activa y automatizada desde febrero de 2026. Se estima que los atacantes lanzaron al menos 659 campañas intensivas de recolección entre el 31 de mayo y el 15 de junio de 2026. Se sospecha el uso de la plataforma de seguridad ofensiva de código abierto basada en IA CyberStrike para optimizar los flujos de intrusión.

Impacto potencial:

- Filtración y descifrado industrial de secretos tecnológicos: La campaña ha recolectado y validado de forma masiva más de 110 millones de credenciales corporativas, desglosadas críticamente en 14.8 millones de credenciales RADIUS, 89 millones de tokens de autenticación MySQL, 924.000 hashes NTLM y 130.000 hashes Kerberos, otorgando llaves maestras de acceso a bases de datos y redes internas.
- Compromiso masivo de la cadena de suministro (Supply Chain): Al enfocar el "bombardeo masivo" hacia pymes y proveedores de servicios de TI, los atacantes buscan explotar las relaciones de confianza técnica de estas empresas para pivotar, saltar el perímetro y comprometer de manera invisible los entornos de producción de sus clientes finales.

- Operación expansiva multi-vendedor: La infraestructura criminal detrás de FortiBleed ha sido diseñada de forma modular; el mismo patrón de ataques de fuerza bruta automatizados se está utilizando de forma concurrente desde el 28 de febrero de 2026 para vulnerar sistemas NAS de Synology, firewalls de Sophos, portales de escritorio remoto RDWeb y VPN SSL de Citrix.
- Comercialización de accesos iniciales y puertas traseras persistentes: Se ha confirmado la inyección de combinaciones idénticas de usuarios y contraseñas repetidas en miles de IPs distintas que funcionan como backdoors clandestinas. Estos paquetes de accesos validados perimetrales se comercializan activamente en la Dark Web por actores como "SantaAd", cotizándose en rangos de entre $30.000 y $60.000 dólares.

Recomendaciones para mitigar el riesgo:

1. Bloqueo y aislamiento de interfaces expuestas: Restringir de manera mandatoria la accesibilidad pública de los paneles de gestión web (UI) y portales de acceso SSL-VPN de FortiGate desde internet. Confinar estos accesos a redes locales de administración aisladas mediante políticas locales (local-in policies) o pasarelas de acceso Zero Trust (ZTNA).

2. Implementación universal y estricta de MFA: Desplegar de forma obligatoria políticas de Autenticación Multifactor (MFA) en la totalidad de las pasarelas externas y conexiones VPN de la organización. Esta contramedida es la única capaz de neutralizar el uso operativo de las credenciales de texto plano que ya han sido filtradas y crackeadas en los repositorios criminales.

3. Caza de indicadores y auditoría de comandos nativos: Configurar alertas específicas en las herramientas de monitoreo orientadas a detectar la ejecución inusual de comandos de diagnóstico de rastreo de red (-diagnose sniffer packet), así como auditorías en sistemas de archivos para aislar ejecutables o scripts vinculados a FortigateSniffer, forticheck o utilidades de la suite CyberStrike.

4. Rotación masiva de secretos y endurecimiento del algoritmo de hashing: Restablecer contraseñas, actualizar a FortiOS (7.2.11, 7.4.8 y 7.6.1) y forzar la migración de hashes SHA-256 a PBKDF2 mediante login-lockout-upon-weaker-encryption.

Prioridad: Urgente.

Ampliar Información:

- https://thehackernews.com/2026/06/fortibleed-targeted-fortigate-firewalls.html
- https://blog.segu-info.com.ar/2026/06/fortibleed-detalles-de-la-operacion-de.html
- https://ciberseguridadegalicia.gal/es/ciberseguridad-al-dia/alertas/campana-fortibleed-compromiso-masivo-de-credenciales-en-dispositivos-fortinet-expuestos-internet
- https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/comunicacion/noticias/fortibleed-campana-masiva-verificacion-credenciales-afecta-dispositivos
- https://fixear.net/noticias/miles-de-dispositivos-fortigate-expuestos-y-la-historia-detras-de-fortibleed
- https://unaaldia.hispasec.com/cisa-urge-a-blindar-dispositivos-fortinet-tras-la-filtracion-fortibleed/
- https://www.euskadi.eus/noticia/2026/fortibleed-75-000-firewalls-fortinet-comprometidos-a-nivel-mundial/web01-ejeduki/es/