GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °4225

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	0	1
MALWARE	0	0	1
NOTICIAS DE CIBERSEGURIDAD	0	0	1

VULNERABILIDADES

CVE-2025-58325 / CVE-2025-49201 / CVE-2025-57740 — FORTINET (EJECUCIÓN DE COMANDOS, BYPASS DE AUTENTICACIÓN Y DESBORDAMIENTO DE MEMORIA HEAP)

El 14 de octubre de 2025, Fortinet publicó un extenso boletín de seguridad que agrupa más de una docena de vulnerabilidades que afectan a su ecosistema de productos, incluyendo FortiOS, FortiProxy, FortiPAM, FortiSwitchManager, FortiAnalyzer y FortiManager.

Entre las más destacadas se encuentra CVE-2025-58325, una vulnerabilidad de tipo Incorrect Provision of Specified Functionality (CWE-684) que permite a un atacante autenticado ejecutar comandos arbitrarios desde la CLI de FortiOS, elevando privilegios y comprometiendo el dispositivo.

Asimismo, la falla CVE-2025-49201 afecta a FortiPAM y FortiSwitchManager, donde una debilidad en el mecanismo de autenticación (CWE-1390) posibilita ataques de fuerza bruta

capaces de eludir controles de acceso, exponiendo consolas administrativas a accesos no autorizados.

Otra vulnerabilidad relevante, CVE-2025-57740, corresponde a un heap overflow autenticado en los marcadores SSL-VPN, presente en FortiOS, FortiProxy y FortiPAM. Aunque catalogada como de severidad media, su explotación podría derivar en ejecución de código o denegación de servicio dentro de sesiones legítimas de VPN.

El resto de los hallazgos incluyen fallas de autorización indebida, exposición de información sensible, validación insuficiente de certificados, y open redirect/XSS, que en conjunto elevan el riesgo operativo en infraestructuras corporativas que dependen de Fortinet como perímetro de seguridad.

Resumen técnico:

- CVE-2025-58325 — Incorrect Provision of Specified Functionality (CWE-684): vulnerabilidad en el componente CLI de FortiOS que permite a un usuario autenticado con privilegios administrativos ejecutar comandos arbitrarios en el sistema, elevando privilegios más allá de lo esperado.
- CVE-2025-49201 — Weak Authentication (CWE-1390): debilidad en los componentes WAD/GUI de FortiPAM y FortiSwitchManager que posibilita ataques de fuerza bruta y bypass de autenticación en consolas de administración.
- CVE-2025-57740 — Heap-based Buffer Overflow (CWE-122): desbordamiento de memoria en el módulo SSL-VPN (RDP bookmarks) de FortiOS, FortiPAM y FortiProxy, que podría permitir ejecución de código o denegación de servicio autenticada.
- Otras vulnerabilidades publicadas el 14 de octubre de 2025 incluyen fallos de exposición de información sensible, validación insuficiente de certificados y autorizaciones indebidas en FortiManager, FortiAnalyzer y FortiSRA.
- Productos afectados: FortiOS, FortiProxy, FortiPAM, FortiSwitchManager, FortiAnalyzer, FortiManager, FortiSASE, FortiWeb, FortiMail y FortiNDR — en versiones comprendidas entre las ramas 7.0.x y 7.6.x.

Impacto potencial:

- Ejecución de comandos privilegiados en appliances Fortinet (FortiGate, FortiProxy, FortiPAM).
- Acceso no autorizado a consolas de administración y servicios críticos.
- Denegación de servicio o corrupción de memoria en módulos SSL-VPN.
- Exposición de datos sensibles en registros o tráfico administrativo.
- Posible escalamiento lateral o compromiso total del entorno de red.

Recomendaciones de mitigación:

1. Actualizar inmediatamente a versiones corregidas: FortiOS: 7.6.3 / 7.4.9 / 7.2.11 / 7.0.16 o superior. FortiPAM: 1.5.1 o 1.4.3 o superior. FortiProxy: 7.6.3 o superior. Y FortiSwitchManager: 7.2.5 o superior.
2. Restringir acceso al CLI y portales administrativos a redes seguras.
3. Habilitar autenticación multifactor (MFA) en cuentas privilegiadas.
4. Revisar registros de comandos y accesos por actividad anómala.
5. Deshabilitar temporalmente funciones SSL-VPN no críticas hasta aplicar los parches.

Prioridad: Crítica.

Ampliar Información:

- https://www.fortiguard.com/psirt
- https://cybersecuritynews.com/fortios-cli-command-bypass-vulnerability/
- https://gbhackers.com/fortios-cli-bypass-flaw/
- https://gbhackers.com/fortipam-fortiswitch-manager-flaw/
- https://cybersecuritynews.com/fortipam-and-fortiswitch-manager-vulnerability/
- https://cyberpress.org/fortios-cli-command-bypass-flaw/

CVE-2025-5947 — SERVICE FINDER (WORDPRESS) (BYPASS DE AUTENTICACIÓN / TOMA DE SESIÓN ADMIN)

El plugin Service Finder Bookings, empaquetado con el tema Service Finder, presenta una vulnerabilidad crítica de bypass de autenticación que permite a un atacante no autenticado obtener la sesión de cualquier usuario, incluidos administradores, mediante la manipulación de la función service_finder_switch_back() y valores de cookie no validados. El fallo está siendo explotado activamente desde agosto de 2025 y pone en riesgo miles de sitios WordPress que aún usan versiones ≤ 6.0.

Resumen técnico:

- CVE-2025-5947 (CVSS 9.8) — autorización bypass vía cookie en la función service_finder_switch_back() del plugin Service Finder Bookings.
- El plugin no valida correctamente el valor de la cookie/parametro usado para el "account switch", lo que permite forzar el inicio de sesión como cualquier usuario sin credenciales.
- La explotación se realiza mediante peticiones HTTP construidas que incluyen el parámetro switch_back o la cookie manipulada; no requiere interacción previa ni autenticación.
- Se ha observado explotación masiva automatizada (escaneo + solicitudes repetidas) desde al menos el 1 de agosto de 2025, con miles de intentos detectados.
- Afecta a todas las versiones hasta la 6.0; la corrección fue publicada en la versión 6.1 (17-jul-2025).
- IPs observadas atacando la funcionalidad switch_back: 5[.]189[.]221[.]98, 185[.]109[.]21[.]157, 192[.]121[.]16[.]196, 194[.]68[.]32[.]71 y 178[.]125[.]204[.]198

Impacto potencial:

- Compromiso completo de sitios WordPress afectados (control administrativo).
- Instalación de web shells, backdoors y persistencia en /wp-content/.
- Uso de sitios comprometidos para hosting de phishing, distribución de malware, SEO poisoning o pivote hacia redes internas.
- Robo de credenciales de usuarios y exfiltración de datos.
- Daño reputacional, pérdida de disponibilidad y riesgos regulatorios por exposición de datos.

Recomendaciones de mitigación:

1. Actualizar inmediata y obligatoriamente el plugin/tema Service Finder Bookings a la versión 6.1 o superior.
2. Si la actualización no es posible de inmediato, desactivar o eliminar el plugin/tema vulnerable y aislar el sitio del público.
3. Revisar y rotar credenciales de cuentas administrativas tras la remediación.
4. Buscar y eliminar web shells, plugins/temas modificados y archivos PHP inusuales en /wp-content/uploads/, /wp-content/themes/ y /wp-content/plugins/.
5. Implementar WAF / virtual patching con reglas que bloqueen patrones switch_back y peticiones anómalas mientras se parchea.
6. Habilitar MFA en todas las cuentas administrativas y limitar accesos por IP (whitelisting) cuando sea posible.
7. Auditar logs de acceso (requests con switch_back, creación de usuarios, cambios de plugins, uploads .php) y realizar hunting por actividad anómala.
8. Mantener copias de seguridad verificadas y playbook de respuesta para restauración en caso de compromiso.

Prioridad: Crítica

Ampliar Información:

- https://portal.cci-entel.cl/Threat_Intelligence/Boletines/2348
- https://csirt.telconet.net/comunicacion/noticias-seguridad/fallo-critico-en-plugin-para-wordpress-permite-a-atacantes-tomar-control-total-del-sitio/
- https://www.cve.org/CVERecord?id=CVE-2025-5947
- https://thehackernews.com/2025/10/critical-exploit-lets-hackers-bypass.html

CVE-2025-11371 — GLADINET CENTRESTACK / TRIOFOX (LFI SIN AUTENTICACIÓN — EXPLOTACIÓN ACTIVA)

Una vulnerabilidad crítica, actualmente explotada en entornos reales, afecta a las plataformas Gladinet CentreStack y Triofox, utilizadas para sincronización y acceso remoto a archivos en entornos empresariales.

El fallo, identificado como CVE-2025-11371 (CVSS 6.1), permite a un atacante no autenticado leer archivos arbitrarios del servidor, incluido el archivo Web.config, desde el cual puede extraer la machineKey de ASP.NET y escalar a ejecución remota de código (RCE) mediante deserialización insegura de ViewState.

Resumen técnico:

- Tipo: LFI (Local File Inclusion) no autenticado.
- Vector: Explotación del handler “temp” en el archivo UploadDownloadProxy\Web.config.
- Efecto: Permite acceder remotamente al contenido de archivos locales sin autenticación, extrayendo el machine key usado para firmar ViewState.
- Cadena de explotación: El atacante accede al endpoint vulnerable y solicita lectura de /Web.config, bbtiene la machineKey almacenada localmente, con esta clave,

construye un payload ViewState malicioso firmado y provoca deserialización insegura, ejecutando comandos de forma remota con privilegios del servidor IIS.
- La explotación fue observada por Huntress SOC el 27 de septiembre de 2025, afectando al menos a tres clientes.
- A la fecha, no existe parche oficial, aunque el fabricante confirmó estar desarrollando uno y publicó una mitigación temporal.

Impacto potencial:

- Acceso remoto a archivos sensibles (credenciales, configuraciones, llaves de aplicación).
- Ejecución remota de código (RCE) mediante ViewState forjado.
- Compromiso total del servidor y movimiento lateral hacia otros sistemas.
- Posible instalación de RATs o backdoors persistentes.
- Riesgo para MSP, empresas de archivos en la nube y entornos corporativos auto-hospedados.

Recomendaciones de mitigación:

1. Deshabilitar el handler “temp” en el archivo: C:\Program Files (x86)\Gladinet Cloud Enterprise\UploadDownloadProxy\Web.config
2. Restringir acceso a las rutas /UploadDownloadProxy/ desde Internet público.
3. Revisar logs del servidor IIS por solicitudes sospechosas o lectura de archivos locales.
4. Implementar monitoreo de integridad sobre Web.config y tráfico ViewState.
5. Mantener segmentación de red, restringiendo acceso a instancias de CentreStack y Triofox.
6. Aplicar parches de seguridad tan pronto el fabricante publique actualización oficial.
7. Comunicar a clientes y proveedores el riesgo asociado a instalaciones sin aislamiento.

Prioridad: Urgente.

Ampliar Información:

- https://www.huntress.com/blog/gladinet-centrestack-triofox-local-file-inclusion-flaw
- https://www.helpnetsecurity.com/2025/10/10/gladinet-centrestack-vulnerability-exploited-cve-2025-11371/
- https://thehackernews.com/2025/10/from-lfi-to-rce-active-exploitation.html

MALWARE

CHAOSBOT — NUEVO BACKDOOR EN RUST USA DISCORD COMO CANAL DE COMANDO Y CONTROL

Investigadores de eSentire Threat Response Unit (TRU) descubrieron una nueva cepa de malware escrita en Rust, denominada ChaosBot, que utiliza los servicios legítimos de Discord como infraestructura de Comando y Control (C2).
El backdoor fue detectado a finales de septiembre de 2025 en un entorno del sector financiero, donde los atacantes habían obtenido acceso mediante credenciales VPN y cuentas de Active Directory sobre-privilegiadas.
El malware destaca por su capacidad para ejecutar comandos remotos, exfiltrar información y mantener persistencia dentro de redes comprometidas, utilizando canales de Discord como interfaz operativa.

Resumen técnico:

- Lenguaje: Rust.
- C2: Discord API (canales privados y tokens embebidos).
- Módulo principal: msedge_elf.dll — cargado mediante DLL sideloading con el binario legítimo identity_helper.exe.

- Métodos de infección: Uso de credenciales comprometidas en CiscoVPN/AD y Campañas de phishing con archivos .LNK maliciosos que ejecutan PowerShell y descargan ChaosBot.
- Funciones principales: shell: ejecutar comandos PowerShell, download / upload: transferir archivos entre víctima y C2 y scr: capturar pantallazos del sistema.
- Persistencia: despliegue de Fast Reverse Proxy (FRP) y tentativa de túneles con Visual Studio Code.
- Evasión: Parches en ntdll!EtwEventWrite para neutralizar Event Tracing for Windows (ETW) y Detección de entornos virtualizados (VMWare, VirtualBox) mediante análisis de direcciones MAC.

Impacto potencial:

- Uso de canales de Discord denominados según el nombre del host infectado (ejemplo: Host-<PCNAME>).
- Comandos y resultados se transfieren directamente en formato texto o imagen dentro del canal.
- Operadores identificados: chaos_00019 y lovebb0024 (cuentas Discord activas desde 2024).
- Capacidad para establecer túneles reversos (FRP) hacia infraestructura alojada en AWS Hong Kong (18.162.110[.]113).
- Relación técnica con el ransomware Chaos-C++, el cual incorpora borrado destructivo de archivos y secuestro de portapapeles para robo de criptomonedas.

Recomendaciones de mitigación:

1. Bloquear tráfico saliente hacia Discord (API/CDN) desde sistemas corporativos o servidores.
2. Monitorear procesos PowerShell o mshta.exe ejecutados tras la apertura de archivos .LNK.
3. Detectar DLL sideloading: generar alerta si identity_helper.exe carga msedge_elf.dll.
4. Revisar logs por descargas o ejecución de FRP (node.exe/node.ini) en rutas públicas.
5. Rotar credenciales de cuentas de servicio o VPN sospechosas y revisar accesos RDP/WMI.
6. Reforzar MFA y segmentación para cuentas administrativas.
7. Bloquear IP 18.162.110[.]113 y otros endpoints asociados.

Prioridad: Urgente.

Ampliar Información:

- https://devel.group/blog/el-malware-chaosbot-utiliza-canales-de-discord-para-tomar-el-control-de-las-computadoras/
- https://www.broadcom.com/support/security-center/protection-bulletin/chaosbot-hiding-on-your-system-and-communicating-through-discord
- https://csirtasobancaria.com/nueva-actividad-de-qilin-ransomware/campana-activa-distribuye-el-rat-xworm-v6/nueva-variante-de-ransomware-denominada-obscura/nueva-campana-de-snake-keylogger/nuevo-backdoor-denominado-chaosbot-ejecuta-ordenes-via-powershell
- https://thehackernews.com/2025/10/new-rust-based-malware-chaosbot-hijacks.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

F5 SUFRE COMPROMISO INTERNO Y FILTRACIÓN DE CÓDIGO FUENTE DE BIG-IP ATRIBUIDO A UN ACTOR ESTATAL

La empresa estadounidense F5 Networks confirmó una intrusión en su entorno interno atribuida a un actor estatal altamente sofisticado, que logró mantener acceso persistente a sus sistemas de desarrollo y exfiltrar fragmentos del código fuente de BIG-IP, junto con información sobre vulnerabilidades aún no divulgadas.

El incidente, descubierto en agosto de 2025 y revelado públicamente el 15 de octubre, representa uno de los compromisos más graves registrados por un proveedor de infraestructura crítica de red en los últimos años.

Aunque F5 aseguró que no existen indicios de explotación activa ni de afectación a la cadena de suministro, el hecho de que el código fuente y configuraciones de clientes

hayan sido exfiltrados plantea un riesgo significativo para entornos empresariales y gubernamentales que dependen de sus productos.

Resumen técnico:

- Intrusión atribuida a un actor estatal con capacidades avanzadas de persistencia y evasión.
- Acceso prolongado a los entornos de desarrollo de BIG-IP y plataformas de gestión de conocimiento.
- Exfiltración confirmada de código fuente y detalles técnicos de vulnerabilidades en investigación.
- No se detectó manipulación de la cadena de suministro, según auditorías independientes de NCC Group e IOActive.
- No hubo acceso a los sistemas CRM, financieros ni de soporte técnico, aunque un porcentaje menor de clientes podría haber sido afectado por filtración de configuraciones.
- F5 trabajó con Google Mandiant y CrowdStrike para contención, rotación de credenciales y endurecimiento de controles.
- Se publicaron actualizaciones de seguridad para BIG-IP, F5OS, BIG-IQ, BIG-IP Next (Kubernetes) y APM clients.
- El ataque refuerza la tendencia de compromisos dirigidos a proveedores de software de red, buscando acceso a entornos críticos mediante la explotación de la cadena de confianza.

Impacto potencial:

- Exposición de componentes internos que podrían facilitar vulnerabilidades futuras o exploits dirigidos.
- Riesgo de ataques de ingeniería inversa sobre el código exfiltrado para descubrir fallas aún no parcheadas.

- Compromiso de confianza en el ecosistema F5, afectando tanto clientes empresariales como agencias gubernamentales.
- Posible uso de la información sustraída para campañas de espionaje o desarrollo de exploits contra entornos BIG-IP y derivados.
- Relevancia geopolítica: la atribución a un actor estatal sugiere interés estratégico en infraestructura crítica y telecomunicaciones.

Recomendaciones para mitigar el riesgo:

- Actualizar inmediatamente todos los productos F5 afectados a las versiones publicadas en el Boletín de Seguridad de octubre 2025.
- Revisar credenciales y políticas de acceso asociadas a consolas de administración BIG-IP y portales F5.
- Integrar logs de BIG-IP al SIEM corporativo y monitorear intentos de autenticación o cambios de configuración inusuales.
- Aplicar las guías de hardening oficiales de F5 e implementar las verificaciones automáticas mediante iHealth Diagnostic Tool.
- Realizar escaneos de vulnerabilidades específicos en appliances F5 y monitorear IOC asociados.
- Mantener comunicación con el soporte oficial de F5 para recibir alertas personalizadas y validación de integridad.

Prioridad: Importante.

Ampliar Información:

- https://www.geekwire.com/2025/f5-discloses-major-security-breach-linked-to-nation-state-hackers/
- https://my.f5.com/manage/s/article/K000154696
- https://thehackernews.com/2025/10/f5-breach-exposes-big-ip-source-code.html