GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °0326

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

BOLETÍN CIBERSEGURIDAD
SEMANAL EDICIÓN º0326

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	3	0	0
MALWARE	0	1	0
NOTICIAS DE CIBERSEGURIDAD	0	1	0

VULNERABILIDADES

PLUGIN ADVANCED CUSTOM FIELDS: EXTENDED (ACF) — ESCALADA DE PRIVILEGIOS CRÍTICA (CVE-2025-14533)

Se ha descubierto una vulnerabilidad de severidad crítica en el popular plugin de WordPress "Advanced Custom Fields: Extended", la cual afecta a más de 100,000 sitios web. El fallo permite a atacantes no autenticados obtener privilegios de administrador de forma remota, otorgándoles control total sobre el sitio afectado. La vulnerabilidad es especialmente peligrosa debido a que no requiere credenciales previas para ser explotada.

Resumen técnico:

- Identificador principal: CVE-2025-14533.
- Severidad: 9.8 (Crítica).
- Causa raíz: Gestión inadecuada de la función insert_user() que no restringe los roles de usuario durante el registro o modificación.
- Mecanismo de falla: El plugin falla al validar las restricciones de roles en formularios públicos; si un formulario tiene mapeado el campo "role", un atacante puede inyectar el valor "administrator" durante el envío.
- Vector de ataque: Envío de solicitudes maliciosas a través de formularios de creación o actualización de usuarios sin necesidad de interacción por parte de un administrador.
- Versiones del plugin Advanced Custom Fields: Extended hasta la 0.9.2.1 inclusive.

Impacto potencial:

- Toma de control total del sitio (Full Takeover): El atacante puede crearse una cuenta con el rol más alto, permitiéndole modificar cualquier configuración de WordPress.
- Despliegue de malware: Al tener acceso administrativo, el atacante puede subir plugins o temas maliciosos que contengan backdoors para persistencia a largo plazo.
- Exfiltración de datos: Acceso completo a la base de datos de usuarios, clientes, pedidos y cualquier información sensible almacenada en el sitio.
- Inyección de contenido malicioso: Modificación de entradas y páginas existentes para redirigir a los usuarios hacia sitios de phishing o estafas.
- Impacto en la disponibilidad: El atacante puede eliminar contenido, bloquear el acceso a administradores legítimos o borrar completamente el sitio web.

Recomendaciones de mitigación:

1. Actualización inmediata: Migrar de forma urgente a la versión 0.9.2.2 o superior, donde el desarrollador ha implementado las validaciones de seguridad necesarias.
2. Auditoría de usuarios: Revisar la lista de usuarios del sitio en busca de nuevas cuentas con rol de administrador que no hayan sido creadas por el equipo oficial.
3. Revisión de formularios: Inspeccionar los formularios de registro creados con ACF Extended y asegurar que el campo "role" no esté expuesto ni mapeado a entradas del usuario.
4. Implementación de WAF: Utilizar un Firewall de Aplicaciones Web que tenga reglas específicas para bloquear intentos de escalada de privilegios en peticiones POST de WordPress.
5. Monitoreo de logs: Analizar los registros de actividad del servidor para identificar patrones de reconocimiento o intentos de registro automatizados sospechosos.

Prioridad: Crítica.

Ampliar información:

- https://www.techradar.com/pro/security/50-000-wordpress-site-affected-in-major-plugin-security-flaw-heres-how-to-stay-safe
- https://www.thaicert.or.th/en/2026/01/22/critical-acf-extended-plugin-vulnerability-allows-attackers-to-gain-administrator-control-on-over-50000-wordpress-sites/
- https://www.wordfence.com/blog/2026/01/100000-wordpress-sites-affected-by-privilege-escalation-vulnerability-in-advanced-custom-fields-extended-wordpress-plugin/
- https://csirt.telconet.net/comunicacion/boletines-servicios/vulnerabilidad-critica-en-plugin-advanced-custom-fields-extended-de-wordpress-permite-escalada-de-privilegios/

ZOOM NODE MULTIMEDIA ROUTERS (MMR) — VULNERABILIDAD CRÍTICA DE INYECCIÓN DE COMANDOS (CVE-2026-22844)

Zoom ha divulgado una vulnerabilidad de seguridad de máxima gravedad que afecta a sus componentes de Node Multimedia Routers (MMR). Esta falla permite a un participante de una reunión con acceso a la red ejecutar comandos arbitrarios de forma remota, lo que representa una amenaza inmediata para las organizaciones que utilizan despliegues híbridos o de conectores de reuniones.

Resumen técnico:

- Identificador principal: CVE-2026-22844.
- Severidad: 9.9 (Crítica).
- Causa raíz: Inyección de comandos en los componentes de procesamiento de medios del MMR.
- Vector de ataque: Acceso a través de la red; requiere privilegios bajos y no necesita interacción del usuario para su ejecución.
- Versiones afectadas: Módulos de Zoom Node Meetings Hybrid (ZMH) y Meeting Connector (MC) en versiones anteriores a la 5.2.1716.0.
- Alcance del compromiso: El diseño de la falla permite que el impacto se extienda más allá del componente vulnerable, comprometiendo potencialmente toda la infraestructura de Zoom Node.

Impacto potencial:

- Ejecución remota de código (RCE): Posibilidad de ejecutar instrucciones maliciosas en el sistema operativo del router mediante credenciales válidas.
- Control total de la infraestructura: Manipulación de las comunicaciones y acceso a recursos gestionados por el nodo comprometido.
- Movimiento lateral en la red: Uso del router afectado como punto de entrada para atacar otros activos corporativos.
- Exfiltración de información confidencial: Intercepción de datos de sesiones y extracción de configuraciones sensibles.
- Interrupción del servicio (DoS): Deshabilitación de las capacidades de videoconferencia híbrida, afectando la continuidad operativa.

Recomendaciones de mitigación:

1. Actualización prioritaria: Actualizar todos los módulos MMR afectados a la versión 5.2.1716.0 o superior de manera inmediata.
2. Inventario de despliegues: Identificar todas las instancias de Zoom Node Meetings Hybrid y Meeting Connector en el entorno para verificar versiones actuales.
3. Segmentación de red: Aislar la infraestructura de Zoom Node de otros sistemas críticos del centro de datos para contener posibles intentos de explotación.
4. Monitoreo de actividad: Revisar los registros de autenticación y el tráfico de red dirigido a los nodos en busca de patrones de comandos inusuales.
5. Hardening de acceso: Limitar el acceso a las interfaces de gestión de los nodos únicamente a segmentos de red de administración confiables.

Prioridad: Crítica.

Ampliar información:

- https://thehackernews.com/2026/01/zoom-and-gitlab-release-security.html
- https://cyberpress.org/critical-zoom-command-injection-vulnerability/
- https://securityaffairs.com/187165/security/zoom-fixed-critical-node-multimedia-routers-flaw.html
- https://csirt.telconet.net/comunicacion/boletines-servicios/vulnerabilidad-critica-de-inyeccion-de-comandos-en-zoom-node-multimedia-routers-permite-ejecucion-remota/

PRODUCTOS CISCO UNIFIED COMMUNICATIONS — EJECUCIÓN REMOTA DE CÓDIGO (CVE-2026-20045)

Se ha identificado una vulnerabilidad crítica de día cero (Zero-Day) que afecta a múltiples productos de la suite de Comunicaciones Unificadas de Cisco, incluyendo Unified CM y Webex Calling. El fallo, que está siendo explotado activamente en entornos reales, permite a atacantes remotos no autenticados ejecutar comandos arbitrarios con privilegios elevados, comprometiendo la infraestructura de voz y colaboración de la organización.

Resumen técnico:

- Identificador principal: CVE-2026-20045.
- Severidad: 8.2 (Clasificada como Crítica por Cisco debido a la escalación a Root).
- Causa raíz: Validación inadecuada de la entrada suministrada por el usuario en solicitudes HTTP dirigidas a la interfaz de gestión.
- Mecanismo de falla: Un atacante puede enviar una secuencia de solicitudes HTTP diseñadas al puerto de administración web para inyectar comandos directamente en el sistema operativo subyacente.
- Estado de explotación: Confirmada como vulnerabilidad Zero-Day con intentos de explotación activos; incluida recientemente en el catálogo KEV de CISA.
- Versiones afectadas: Afecta a las ramas 12.5, 14 y 15 de Unified CM, Unified CM SME, Unity Connection y Webex Calling Dedicated Instance.

Impacto potencial:

- Escalación de privilegios a Root: El atacante puede elevar rápidamente sus permisos hasta obtener control total del sistema operativo.
- Ejecución de comandos arbitrarios: Posibilidad de ejecutar cualquier instrucción, instalar malware o mecanismos de persistencia.
- Compromiso total de comunicaciones: Intercepción, manipulación o interrupción de servicios de telefonía, mensajería y presencia corporativa.
- Movimiento lateral estratégico: Uso del servidor como punto de pivote para atacar otros sistemas en segmentos de red privilegiados.
- Exfiltración de datos sensibles: Acceso a información crítica como bases de datos de usuarios, registros, configuraciones y certificados de seguridad.

Recomendaciones de mitigación:

1. Actualización inmediata: Aplicar de forma urgente los parches de software (archivos .cop) o migrar a las versiones fijas (14SU5 o 15SU4) según la rama de despliegue.
2. Restricción de interfaces: Deshabilitar la exposición de las interfaces de gestión web hacia redes externas o segmentos de usuarios no autorizados.
3. Control de acceso (ACLs): Implementar listas de control de acceso estrictas para permitir el tráfico HTTP/HTTPS únicamente desde estaciones de trabajo de administración conocidas.
4. Monitoreo de solicitudes HTTP: Configurar el IPS o el SIEM para detectar patrones de solicitudes inusuales o malformadas dirigidas a los puertos de gestión de Cisco (80/443).
5. Auditoría de integridad: Realizar una revisión de cuentas de sistema y procesos activos en busca de indicadores de compromiso (IoC) tras el parcheo.

Prioridad: Crítica.

Ampliar información:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voice-rce-mORhqY4b
- https://thehackernews.com/2026/01/cisco-fixes-actively-exploited-zero-day.html
- https://socradar.io/blog/cve-2026-20045-cisco-unified-communications-0-day/
- https://www.theregister.com/2026/01/22/another_week_another_emergency_patch/

MALWARE

PDFSIDER — BACKDOOR APT CON TÉCNICAS AVANZADAS DE EVASIÓN Y DLL SIDELOADING

PDFSIDER es una variante de malware de tipo Puerta Trasera (Backdoor) recientemente identificada, vinculada a grupos de Amenaza Persistente Avanzada (APT). Se destaca por su capacidad de operar casi enteramente en memoria y utilizar software legítimo como vehículo de infección para eludir sistemas EDR y antivirus modernos. Ha sido detectado en ataques dirigidos contra corporaciones energéticas de la lista Fortune 100, utilizando ingeniería social táctica.

Resumen técnico:

- Vector de infección inicial: Distribución mediante correos de spear-phishing con archivos ZIP que contienen un ejecutable legítimo (ej. "PDF24 App") firmado digitalmente.
- Técnica de ejecución: Utiliza DLL Side-Loading mediante el secuestro del archivo cryptbase.dll. Al ejecutar la aplicación legítima, esta carga la biblioteca maliciosa del atacante en lugar de la del sistema.
- Cifrado C2 de alto nivel: Incorpora la biblioteca criptográfica Botan 3.0.0 configurada con cifrado autenticado AES-256-GCM para asegurar sus comunicaciones de Comando y Control.
- Persistencia y sigilo: Opera principalmente en memoria para minimizar rastros en el disco y utiliza el indicador CREATE_NO_WINDOW para ocultar la ejecución de comandos de shell (cmd.exe).
- Tecnología Anti-Análisis: Implementa una validación del entorno multietapa que utiliza GlobalMemoryStatusEx para detectar máquinas virtuales o sandboxes (mediante el conteo de RAM) y detener su ejecución.

Impacto potencial:

- Acceso persistente y encubierto: Diseñado para espionaje a largo plazo, permitiendo a los atacantes mantener un control silencioso sobre la estación de trabajo comprometida.
- Exfiltración de datos sensible: Capacidad para recolectar información del sistema, credenciales y archivos críticos, enviándolos cifrados a través del puerto DNS 53 para evadir firewalls.
- Control interactivo remoto: Proporciona a los operadores un shell de comandos oculto para ejecutar instrucciones arbitrarias en el endpoint de la víctima.
- Facilitación de Ransomware: Se ha identificado que diversos actores de ransomware están adoptando PDFSIDER como método primario para la entrega de cargas útiles (payloads).
- Evasión de detección: Al utilizar binarios legítimos firmados y técnicas de carga lateral, logra una tasa de detección extremadamente baja en soluciones de seguridad perimetral y de endpoint.

Recomendaciones de mitigación:

1. Monitoreo de carga de DLLs: Configurar reglas de EDR/SIEM para alertar sobre aplicaciones legítimas (como PDF24, VLC, etc.) que carguen bibliotecas desde directorios inusuales como %AppData% o %Temp%.
2. Restricción de herramientas de asistencia: Limitar o supervisar estrictamente el uso de herramientas como QuickAssist, utilizadas frecuentemente por atacantes para ingeniería social.
3. Control de ejecución: Implementar políticas de restricción de software que impidan la ejecución de binarios desconocidos desde carpetas de usuario no administrativas.
4. Análisis de red: Monitorear el tráfico saliente por el puerto 53 (DNS) en busca de volúmenes de datos anómalos que puedan indicar canales de exfiltración C2 cifrados.
5. Validación de procesos: Auditar procesos hijos de aplicaciones de productividad que intenten invocar intérpretes de comandos (cmd.exe o powershell.exe).

Prioridad: Urgente.

Ampliar información:

- https://blog.segu-info.com.ar/2026/01/pdfsider-utiliza-carga-lateral-de-dll.html
- https://www.resecurity.com/blog/article/pdfsider-malware-exploitation-of-dll-side-loading-for-av-and-edr-evasion
- https://securityaffairs.com/187126/malware/pdfsider-malware-exploitation-of-dll-side-loading-for-av-and-edr-evasion.html
- https://www.securityweek.com/apt-grade-pdfsider-malware-used-by-ransomware-groups/amp/

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

ATAQUES AUTOMATIZADOS CONTRA FIREWALLS FORTIGATE — CAMPAÑA DE EXPLOTACIÓN ACTIVA EN SSO

Investigadores de seguridad de Arctic Wolf y Huntress han alertado sobre un nuevo clúster de actividad maliciosa automatizada dirigida a dispositivos FortiGate. La campaña, que se intensificó a partir del 15 de enero de 2026, aprovecha vulnerabilidades en el mecanismo de autenticación de FortiCloud SSO para comprometer firewalls, incluso en versiones de firmware que se consideraban protegidas tras los parches de diciembre.

Resumen técnico:

- Clúster de actividad detectado: Se observa una ola de ataques automatizados que utilizan mensajes SAML manipulados para eludir la autenticación (CVE-2025-59718 / CVE-2025-59719).
- Falla en el parche (Patch Bypass): Múltiples reportes de administradores y firmas de seguridad indican que la explotación persiste en versiones como la 7.4.9, sugiriendo que las correcciones iniciales fueron incompletas.
- Uso de cuentas genéricas: Los atacantes utilizan sistemáticamente la cuenta cloud-init@mail.io para realizar inicios de sesión maliciosos y descargar archivos de configuración del sistema.
- Exfiltración y persistencia: En cuestión de segundos tras el acceso, los actores de amenaza exportan la configuración del firewall y crean cuentas de administrador secundarias (ej. secadmin, itadmin, helpdesk) para asegurar el acceso permanente.
- Escalación de alertas: CISA ha incluido nuevamente estas vulnerabilidades en su catálogo KEV, subrayando la urgencia de aplicar mitigaciones adicionales ante la ineficacia de algunos parches.

Impacto potencial:

- Compromiso total del perímetro: El acceso administrativo mediante SSO otorga al atacante control absoluto sobre las reglas de red y políticas de seguridad del firewall.
- Robo de credenciales en masa: Al descargar los archivos de configuración (config.conf), los atacantes obtienen acceso a los hashes de contraseñas de todos los usuarios locales y secretos de VPN.
- Movimiento lateral automatizado: La rapidez de las acciones (segundos entre el login y la creación de cuentas) indica el uso de scripts avanzados para comprometer redes a gran escala.
- Persistencia invisible: La creación de cuentas con nombres legítimos (como support o backup) permite que el atacante mantenga el control incluso después de un cambio de contraseñas de la cuenta principal.
- Pérdida de confianza en el ciclo de parches: La incertidumbre sobre qué versiones son realmente seguras obliga a las organizaciones a adoptar medidas de mitigación drásticas y manuales.

Recomendaciones para mitigar el riesgo:

1. Desactivación de SSO: Se recomienda encarecidamente deshabilitar la opción de "Allow administrative login using FortiCloud SSO" mediante el comando CLI: config system global -> set admin-forticloud-sso-login disable.
2. Auditoría de logs: Revisar de forma exhaustiva los registros de sistema en busca de inicios de sesión exitosos mediante el método forticloud-sso desde direcciones IP desconocidas.
3. Búsqueda de cuentas anómalas: Verificar la existencia de usuarios administradores creados recientemente con nombres como helpdesk, secadmin, itadmin, support o cloud-init.
4. Restricción de gestión: Limitar el acceso a las interfaces de administración (GUI/SSH) únicamente a redes internas confiables o mediante túneles VPN seguros, eliminando la exposición hacia internet.
5. Rotación de secretos: Si se detecta un compromiso, se debe asumir que todos los hashes de contraseñas han sido exfiltrados; es imperativo rotar todas las credenciales tras asegurar el dispositivo.

Prioridad: Urgente.

Ampliar Información:

- https://arcticwolf.com/resources/blog/arctic-wolf-observes-malicious-configuration-changes-fortinet-fortigate-devices-via-sso-accounts/
- https://www.helpnetsecurity.com/2026/01/21/patched-fortigate-compromised-via-cve-2025-59718/
- https://thehackernews.com/2026/01/automated-fortigate-attacks-exploit.html