GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °0826

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

FORTINET — BYPASS DE AUTENTICACIÓN ADMINISTRATIVA EN FORTICLOUD SSO (FG-IR-26-060)

Fortinet ha confirmado la explotación activa de una vulnerabilidad crítica de tipo Zero-Day que afecta a FortiCloud Single Sign-On (SSO). El fallo permite a un atacante obtener acceso administrativo completo a dispositivos registrados en cuentas de terceros mediante una omisión de autenticación por canal alternativo, lo que representa un riesgo extremo para la integridad de la infraestructura.

Resumen técnico:

- Identificador principal: FG-IR-26-060 (Relacionado con el aviso previo FG-IR-25-647).
- Severidad: Crítica (Basado en bypass de autenticación administrativa).
- Causa raíz: Vulnerabilidad de omisión de autenticación mediante una ruta o canal alternativo (CWE-288).
- Mecanismo de falla: Un atacante con una cuenta FortiCloud maliciosa puede autenticarse vía SSO en dispositivos ajenos si la función está habilitada, obteniendo privilegios de superusuario.
- Estado de explotación: Explotación activa confirmada. Se ha detectado la creación de usuarios administradores locales como audit, backup, itadmin, support, entre otros.
- Versiones afectadas: FortiOS (7.0 a 7.6), FortiManager (7.0 a 7.6), FortiAnalyzer (7.0 a 7.6) y FortiProxy (7.0 a 7.6).

Impacto potencial:

- Compromiso total del dispositivo: El atacante obtiene acceso administrativo completo, permitiendo la modificación de cualquier regla de seguridad o política de red.
- Persistencia a largo plazo: Los atacantes están creando múltiples cuentas locales (ej. security, svcadmin) para mantener el control incluso si se deshabilita el SSO.
- Exfiltración de configuración y secretos: Se ha documentado la descarga de archivos de configuración completos, exponiendo credenciales, llaves y topologías.
- Riesgo de movimiento lateral: El acceso al firewall perimetral actúa como puerta de enlace para ataques contra el resto de la red interna.

Recomendaciones de mitigación:

1. Deshabilitar FortiCloud SSO: Si no es indispensable, ejecutar el comando set admin-forticloud-sso-login disable (en FortiOS/Proxy) o set forticloud-sso disable (en FMG/FAZ).
2. Actualización inmediata de Firmware: Migrar a las versiones corregidas (ej. FortiOS 7.6.6, 7.4.11, 7.2.13 o 7.0.19) utilizando la herramienta Fortinet Upgrade Tool.
3. Auditoría de logs de acceso y cuentas: Buscar inicios de sesión exitosos con logid=0100032001 y creaciones de usuarios sospechosos (ej. backupadmin, remoteadmin) con logid=0100044547.
4. Restricción de acceso administrativo: Implementar local-in policies para permitir el acceso a la gestión del dispositivo únicamente desde direcciones IP de administración confiables.

Prioridad: Crítica.

Ampliar información:

- https://blog.segu-info.com.ar/2026/02/fortinet-avisa-de-nuevo-de-la.html
- **https://www.fortiguard.com/psirt/FG-IR-26-076**

BEYONDTRUST — EJECUCIÓN REMOTA DE CÓDIGO PRE-AUTENTICACIÓN (CVE-2026-1731)

Se ha detectado la explotación activa de una vulnerabilidad crítica en las soluciones Remote Support (RS) y Privileged Remote Access (PRA) de BeyondTrust. El fallo permite a un atacante remoto no autenticado ejecutar comandos arbitrarios en el sistema operativo a través del componente de gestión de WebSockets. Debido a su facilidad de explotación y severidad, CISA ha incluido este fallo en su catálogo KEV, vinculándolo además con operaciones de ransomware.

Resumen técnico:

- Identificador principal: CVE-2026-1731.
- Severidad: 9.9 (Crítica) en la escala CVSSv4.
- Causa raíz: Inyección de comandos del sistema operativo (CWE-78) en el script thin-scc-wrapper.
- Mecanismo de falla: El componente falla al sanitizar el parámetro remoteVersion durante el apretón de manos (handshake) de WebSocket, permitiendo que el intérprete Bash evalúe y ejecute comandos embebidos mediante sustitución $(comando).
- Estado de explotación: Confirmada en sectores financiero, salud y tecnología. Se ha observado el despliegue de backdoors como SparkRAT y VShell.
- Versiones afectadas: Remote Support (25.3.1 y anteriores) y Privileged Remote Access (24.3.4 y anteriores).

Impacto potencial:

- Compromiso total del sistema: El acceso pre-autenticación otorga control sobre la configuración del appliance, sesiones gestionadas y tráfico de red sin interacción del usuario.
- Persistencia mediante Web Shells: Los atacantes están instalando múltiples puertas traseras (ej. aws.php, file_save.php) para ejecutar código PHP y comandos de sistema de forma encubierta.
- Secuestro de cuentas administrativas: Se ha documentado el uso de scripts en Python para suplantar temporalmente al administrador principal (User ID 1) modificando directamente la base de datos de autenticación.
- Exfiltración de activos sensibles: Los actores de amenaza están realizando volcados completos de bases de datos PostgreSQL y robando archivos de configuración que contienen secretos corporativos.

Recomendaciones de mitigación:

1. Actualización urgente de parches: Aplicar de inmediato las versiones corregidas RS 25.3.2 o PRA 25.1 (o parches equivalentes BT26-02-RS/PRA) según la ruta de actualización del fabricante.
2. Aislamiento de interfaces de gestión: Restringir el acceso a los appliances de BeyondTrust únicamente a través de redes VPN empresariales o gateways de acceso Zero Trust (ZTNA), evitando la exposición directa a Internet.
3. Auditoría de integridad de archivos: Revisar los directorios web y de aplicaciones en busca de scripts inusuales o modificaciones recientes en la configuración de Apache (técnica de config STOMPing).
4. Monitoreo de actividad anómala: Implementar reglas de detección para identificar procesos hijos sospechosos originados por bomgar-scc y conexiones salientes hacia dominios de pruebas OAST (ej. oastify.com).

Prioridad: Crítica.

Ampliar información:

- https://securityaffairs.com/188370/hacking/cve-2026-1731-fuels-ongoing-attacks-on-beyondtrust-remote-access-products.html
- https://www.lumificyber.com/threat-library/beyondtrust-rs-pra-critical-rce-exploited-in-the-wild-cve-2026-1731/
- https://thehackernews.com/2026/02/beyondtrust-flaw-used-for-web-shells.html
- https://unit42.paloaltonetworks.com/beyondtrust-cve-2026-1731/

ANTHROPIC CLAUDE CODE — RCE Y EXFILTRACIÓN DE API KEYS (CVE-2025-59536, CVE-2026-21852)

Investigadores de Check Point Research han revelado múltiples vulnerabilidades críticas en Claude Code, la herramienta de terminal de Anthropic para codificación asistida por IA. Los fallos permiten a un atacante ejecutar comandos arbitrarios y robar credenciales de API con solo clonar y abrir un repositorio malicioso. Este vector de ataque, denominado "Clone-and-Pwn", convierte los archivos de configuración del proyecto en una capa de ejecución peligrosa que actúa antes de que el usuario otorgue su confianza al directorio.

Resumen técnico:

- Identificadores principales: CVE-2025-59536 y CVE-2026-21852.
- Severidad: 8.7 (Crítica) para los fallos de RCE.
- Causa raíz: Ejecución insegura de ganchos (hooks) y falta de validación en la inicialización de servidores MCP y variables de entorno en archivos .claude/settings.json y .mcp.json.
- Mecanismo de falla (RCE): Una condición de carrera durante la inicialización permite que comandos definidos en el proyecto se ejecuten automáticamente antes de que se presente el diálogo de "confianza" al usuario.
- Mecanismo de falla (Exfiltración): Al sobrescribir la variable ANTHROPIC_BASE_URL en la configuración del repo, el tráfico autenticado se redirige a un servidor del atacante, capturando la API Key en el encabezado.
- Estado de explotación: Divulgación pública el 25 de febrero de 2026. Los parches han sido aplicados en versiones recientes (2.0.65+).

Impacto potencial:

- Ejecución de código arbitrario: Un atacante puede obtener una reverse shell en la máquina del desarrollador simplemente logrando que este inicialice el agente de IA en una carpeta comprometida.
- Robo de identidad de API: La exfiltración silenciosa de la API Key permite al atacante acceder a los archivos de proyectos compartidos en el Workspace de Claude de la organización.
- Compromiso de la cadena de suministro: Un único contribuyente malicioso puede inyectar estas configuraciones en repositorios corporativos internos, afectando a todo el equipo de desarrollo.
- Fraude y costos imprevistos: El uso de las llaves robadas permite realizar consultas masivas a la API con cargo a la cuenta de la víctima o agotar las cuotas de almacenamiento de 100 GB del Workspace.

Recomendaciones de mitigación:

1. Actualización inmediata de la herramienta: Verificar que claude-code esté actualizado a la versión 2.0.65 o superior, donde se han reforzado los controles de confianza y el orden de ejecución.
2. Auditoría de configuraciones de agentes: Inspeccionar los directorios .claude/ y .mcp/ en busca de archivos settings.json que contengan comandos sospechosos en la sección de hooks o servidores MCP.
3. Control de tráfico de red: Implementar reglas en el firewall de red para bloquear conexiones salientes desde terminales de desarrollo hacia dominios no oficiales que intenten suplantar las APIs de Anthropic.
4. Rotación preventiva de API Keys: Si se ha interactuado con repositorios externos o no confiables usando Claude Code recientemente, se recomienda rotar las llaves de API de inmediato desde la consola de Anthropic.

Prioridad: Crítica.

Ampliar información:

- https://securityaffairs.com/188508/security/untrusted-repositories-turn-claude-code-into-an-attack-vector.html
- https://research.checkpoint.com/2026/rce-and-api-token-exfiltration-through-claude-code-project-files-cve-2025-59536/
- https://threatlandscape.io/blog/analyzing-cve-2025-59536-cve-2026-21852-agent-configuration-risks
- https://thehackernews.com/2026/02/claude-code-flaws-allow-remote-code.html

MALWARE

MALWARE — MASSIV: TROYANO BANCARIO Y DE TOMA DE CONTROL (DTO) EN ANDROID

Investigadores de ciberseguridad han alertado sobre Massiv, un nuevo y sofisticado troyano bancario para Android diseñado para la toma de control total del dispositivo (Device Takeover - DTO). Este malware se distribuye principalmente a través de aplicaciones falsas de IPTV gratuitas (fuera de la Play Store), aprovechando el interés de los usuarios por contenidos premium como fútbol o series. Su objetivo principal es el robo de credenciales bancarias y la ejecución de transacciones fraudulentas de forma encubierta.

Resumen técnico:

- Tipo de amenaza: Device Takeover Trojan (DTO) / Troyano bancario móvil.
- Vector de infección: Carga lateral (sideloading) de archivos APK maliciosos disfrazados de apps de IPTV (ej. "IPTV24") distribuidos vía SMS o Telegram.
- Técnica de evasión: Una vez instalado, se oculta bajo nombres legítimos como "Google Play Service" y solicita permisos de Accesibilidad para controlar el sistema.
- Mecanismo de control: Utiliza WebSockets para la comunicación con su servidor de Mando y Control (C2), permitiendo el streaming de pantalla mediante la API MediaProjection de Android.
- Persistencia y bypass: Implementa el modo "UI-tree" para extraer texto y coordenadas de la pantalla, logrando evadir las protecciones contra capturas de pantalla de las aplicaciones bancarias.

Impacto potencial:

- Toma de control remota (DTO): Los atacantes pueden interactuar con el teléfono en tiempo real (clics, swipes, apertura de apps) como si lo tuvieran físicamente en sus manos.
- Fraude bancario invisible: El malware activa un modo de "pantalla negra" que oscurece el panel y silencia notificaciones, permitiendo realizar transferencias bancarias mientras el usuario cree que el móvil está apagado.
- Intercepción de 2FA y SMS: Massiv tiene la capacidad de leer y eliminar mensajes SMS, permitiendo capturar códigos de verificación para eludir la autenticación de doble factor de los bancos.
- Modificación del portapapeles: El troyano monitorea el portapapeles para cambiar direcciones de billeteras de criptomonedas o números de cuenta (IBAN) justo antes de que el usuario confirme una operación.

Recomendaciones de mitigación:

1. Prohibir el Sideloading: Restringir la instalación de aplicaciones desde fuentes desconocidas o repositorios externos a Google Play Store, especialmente aquellas que prometen servicios de streaming gratuitos.
2. Auditoría de Permisos de Accesibilidad: Revisar periódicamente en los ajustes del dispositivo qué aplicaciones tienen acceso a los "Servicios de Accesibilidad" y revocarlo a cualquier app de origen dudoso.
3. Monitoreo de Consumo de Batería y Datos: Desconfiar de aplicaciones que muestren un consumo inusual de batería o tráfico de datos en segundo plano, lo cual es indicativo de actividad de control remoto.
4. Uso de MFA no basado en SMS: Siempre que la entidad financiera lo permita, priorizar el uso de aplicaciones de autenticación o llaves físicas (FIDO) en lugar de códigos vía SMS que pueden ser interceptados.

Prioridad: Urgente.

Ampliar información:

- https://thehackernews.com/2026/02/fake-iptv-apps-spread-massiv-android.html
- https://www.fayerwayer.com/internet/2026/02/24/esta-app-para-ver-tv-online-gratis-es-en-realidad-un-virus-bastante-peligroso/
- https://blog.ethergroup.mx/posts/Massiv-tu-app-de-IPTV-te-quita-tus-ahorros/
- https://roams.es/actualidad/alarmas-seguridad/iptv-futbol-pirata-series-gratis-malware-massiv-cuenta-a-cero/

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

ACTOR ASISTIDO POR IA COMPROMETE MÁS DE 600 DISPOSITIVOS FORTIGATE

Amazon Threat Intelligence ha revelado una campaña masiva donde un actor de amenazas rusoparlante utilizó múltiples servicios comerciales de IA Generativa para comprometer más de 600 dispositivos FortiGate en 55 países. Lo más relevante de este caso es que el atacante, con capacidades técnicas limitadas, logró una escala operativa de tipo APT gracias al uso de la IA como "cadena de montaje" para automatizar el ciclo de ataque, desde el reconocimiento hasta el despliegue de malware.

Resumen técnico:

- Periodo de actividad: Del 11 de enero al 18 de febrero de 2026 (Investigación publicada el 20 de febrero).
- Alcance geográfico: Dispositivos distribuidos globalmente, con concentraciones significativas en Latinoamérica, el Sudeste Asiático y África Occidental.
- Vector de acceso: No se explotaron vulnerabilidades de día cero; el éxito radicó en el escaneo masivo de puertos de gestión expuestos (443, 8443, 10443 y 4443) y el abuso de credenciales débiles con autenticación de un solo factor (SFA).
- Uso de IA: Desarrollo de scripts de reconocimiento en Python/Go, planificación de ataques paso a paso y herramientas para descifrar archivos de configuración robados.
- Infraestructura detectada: Se identificaron las IPs 212.11.64.250 y 185.196.11.225 como origen de los escaneos y host de las herramientas de IA.

Impacto potencial:

- Compromiso a nivel organizacional: El acceso a las configuraciones de FortiGate permitió extraer credenciales SSL-VPN, topologías de red completas y políticas de firewall, facilitando el movimiento lateral.
- Riesgo inminente de Ransomware: Se detectó un enfoque específico en servidores Veeam Backup & Replication para destruir capacidades de recuperación antes de un posible cifrado de datos.
- Vulneración de Active Directory: Uso de ataques DCSync y recolección masiva de hashes NTLM para obtener control total de los dominios internos de las víctimas.
- Persistencia mediante herramientas Open-Source: Despliegue de frameworks como Meterpreter y scripts de PowerShell para mantener el acceso incluso tras intentos de limpieza básicos.

Recomendaciones para mitigar el riesgo:

1. Aislamiento de interfaces de gestión: Asegurar que las interfaces administrativas de FortiGate no sean accesibles desde Internet. Implementar hosts bastión o redes de gestión fuera de banda.
2. Adopción estricta de MFA: Implementar autenticación multifactor obligatoria para todos los accesos administrativos y de VPN (SSL-VPN), eliminando cualquier dependencia de solo contraseña.
3. Rotación y auditoría de credenciales: Cambiar todas las contraseñas administrativas y de usuarios VPN de forma inmediata. Auditar la creación de cuentas locales sospechosas con nombres que imitan servicios legítimos.
4. Protección de la infraestructura de respaldo: Aislar los servidores de backup del acceso general de la red y configurar copias de seguridad inmutables que no puedan ser modificadas ni por administradores comprometidos.

Prioridad: Urgente.

Ampliar Información:

- https://blog.segu-info.com.ar/2026/02/agente-asistido-por-ia-compromete.html
- https://www.darkreading.com/threat-intelligence/600-fortigate-devices-hacked-ai-amateur
- https://www.esecurityplanet.com/threats/aws-threat-intel-finds-600-fortigate-devices-hit/
- https://thehackernews.com/2026/02/ai-assisted-threat-actor-compromises.html
- https://aws.amazon.com/blogs/security/ai-augmented-threat-actor-accesses-fortigate-devices-at-scale/