GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º0226

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	0	1
NOTICIAS DE CIBERSEGURIDAD	0	0	1

VULNERABILIDADES

PLATAFORMA FORTINET FORTISIEM — VULNERABILIDAD CRÍTICA DE RCE SIN AUTENTICACIÓN (CVE-2025-64155)

Fortinet ha publicado correcciones para una falla de seguridad de máxima gravedad en FortiSIEM que permite a un atacante no autenticado ejecutar código de forma remota en instancias vulnerables. El fallo se origina en el manejo inadecuado de solicitudes TCP especialmente diseñadas dirigidas al servicio de monitoreo de la plataforma.

Resumen técnico:

- Identificador principal: CVE-2025-64155.
- Severidad: 9.4 (Crítica).
- Causa raíz: Inyección de comandos del sistema operativo (CWE-78) debido a la neutralización inadecuada de elementos especiales en el servicio phMonitor.
- Mecanismo de falla: El servicio phMonitor (puerto TCP 7900) invoca scripts de shell con parámetros controlados por el usuario, permitiendo la inyección de argumentos mediante curl para realizar escrituras arbitrarias de archivos.
- Vector de ataque: Acceso de red al puerto 7900; no requiere credenciales ni interacción del usuario para la ejecución inicial.
- Versiones afectadas: Versiones de FortiSIEM 6.7.0 a 6.7.10, 7.0.0 a 7.0.4, 7.1.0 a 7.1.8, 7.2.0 a 7.2.6, 7.3.0 a 7.3.4 y la versión 7.4.0.

Impacto potencial:

- Ejecución de comandos no autorizados: Capacidad de ejecutar instrucciones arbitrarias a nivel de sistema operativo en los nodos "Super" y "Worker".
- Escalación de privilegios a Root: Un atacante puede sobrescribir scripts programados (como /opt/charting/redishb.sh) para elevar privilegios de usuario administrador a root mediante tareas cron.
- Compromiso total del dispositivo: Control absoluto sobre la confidencialidad e integridad de los datos almacenados y procesados por el SIEM.
- Persistencia maliciosa: Posibilidad de establecer puertas traseras permanentes y realizar movimientos laterales dentro de la red administrativa.

Recomendaciones de mitigación:

1. Actualización prioritaria: Migrar de forma inmediata a las versiones corregidas: 7.1.9, 7.2.7, 7.3.5, 7.4.1 o superiores según la rama utilizada.
2. Restricción de puertos: Bloquear o limitar el acceso al puerto TCP 7900 (phMonitor) únicamente a redes de gestión interna confiables.
3. Segmentación de red: Aislar el acceso a la interfaz de gestión de FortiSIEM mediante firewalls perimetrales para reducir la superficie de exposición.
4. Auditoría de integridad: Revisar tareas programadas (cron jobs) y registros de phMonitor en busca de ejecuciones anómalas o modificaciones de scripts críticos.

Prioridad: Crítica.

Ampliar información:

- https://www.fortiguard.com/psirt/FG-IR-25-084
- **https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-fortinet-products-could-allow-for-arbitrary-code-execution_2026-003**
- **https://thehackernews.com/2026/01/fortinet-fixes-critical-fortisiem-flaw.html**
- **https://csirt.gob.bo/es/alertas-de-seguridad/cve-2025-64155-inyeccion-remota-de-comandos-no-autenticados-en-fortinet**

TREND MICRO APEX CENTRAL — VULNERABILIDAD CRÍTICA DE RCE CON PRIVILEGIOS SYSTEM (CVE-2025-69258)

Trend Micro ha emitido un parche de urgencia para corregir tres fallos de seguridad en la consola de gestión Apex Central, siendo el más grave una vulnerabilidad de ejecución remota de código (RCE). El defecto permite a un atacante no autenticado cargar una

biblioteca dinámica (DLL) maliciosa en un ejecutable clave del sistema, logrando el control total del servidor con los máximos privilegios posibles.

Resumen técnico:

- Identificador principal: CVE-2025-69258 (RCE), CVE-2025-69259 y CVE-2025-69260 (DoS).
- Severidad: 9.8 (Crítica).
- Causa raíz: Uso inseguro de la función LoadLibraryEX en el componente MsgReceiver.exe.
- Mecanismo de falla: El proceso vulnerable escucha en el puerto TCP 20001; al recibir un mensaje específico (0x0a8d), el sistema carga una DLL controlada por el atacante sin validación previa.
- Vector de ataque: Acceso remoto a través de la red hacia el puerto del servicio; no requiere autenticación ni interacción del usuario.
- Versiones afectadas: Apex Central (on-premise) en Windows, todas las versiones anteriores a la Build 7190.

Impacto potencial:

- Ejecución de código como SYSTEM: Capacidad de ejecutar instrucciones arbitrarias con los privilegios más altos del sistema operativo Windows.
- Toma de control de la gestión: Un atacante exitoso puede manipular políticas de seguridad, exfiltrar información sensible o desactivar la protección antivirus en toda la red.

- Denegación de Servicio (DoS): Los fallos adicionales permiten provocar la caída del servicio MsgReceiver.exe mediante lecturas fuera de límites o valores nulos no verificados.
- Distribución de malware: El servidor comprometido puede ser utilizado para orquestar ataques internos o distribuir software malicioso a gran escala dentro de la organización.

Recomendaciones de mitigación:

1. Actualización inmediata: Instalar de forma urgente el parche crítico Build 7190 o versiones superiores.
2. Restricción por Firewall: Limitar el acceso al puerto TCP 20001 únicamente a direcciones IP conocidas y redes de administración confiables.
3. Seguridad perimetral: Evitar la exposición directa de los servicios de Apex Central a la red pública (Internet).
4. Monitoreo de anomalías: Implementar soluciones EDR para detectar la carga de archivos DLL no autorizados o comportamientos sospechosos en el proceso MsgReceiver.exe.

Prioridad: Crítica.

Ampliar información:

- https://success.trendmicro.com/en-US/solution/KA-0022071
- https://unaaldia.hispasec.com/2026/01/parche-urgente-para-apex-central-trend-micro-resuelve-vulnerabilidad-critica-de-ejecucion-remota.html
- https://securityaffairs.com/186733/hacking/trend-micro-fixed-a-remote-code-execution-in-apex-central.html

- https://thehackernews.com/2026/01/trend-micro-apex-central-rce-flaw.html

VMWARE ESXI — EXPLOTACIÓN ACTIVA DE ZERO-DAYS PARA ESCAPE DE MÁQUINA VIRTUAL (TOOLKIT MAESTRO)

Se ha detectado una campaña de ciberataques sofisticados dirigidos contra hipervisores VMware ESXi. Los atacantes utilizan un conjunto de vulnerabilidades críticas, encadenadas a través de un kit de herramientas denominado "MAESTRO", para romper el aislamiento de las máquinas virtuales (VM) y ejecutar código directamente en el sistema host (hipervisor).

Resumen técnico:

- Identificadores principales: CVE-2025-22224 (9.3), CVE-2025-22225 (8.2) y CVE-2025-22226 (7.1).
- Severidad: Crítica (en conjunto permiten el compromiso total del entorno de virtualización).
- Causa raíz: Fallos de lectura fuera de límites en HGFS, corrupción de memoria en la interfaz VMCI y escritura arbitraria en el sandbox de VMX.
- Mecanismo de falla: El toolkit MAESTRO automatiza la desactivación de controladores, carga un driver de kernel no firmado para identificar la versión de ESXi y despliega un backdoor ELF (VSOCKpuppet) que opera sobre sockets virtuales (VSOCK).
- Vector de ataque: Requiere acceso previo con privilegios administrativos en una VM invitada o el compromiso inicial de dispositivos perimetrales (como VPN SonicWall) para pivotar hacia el entorno virtual.
- Versiones afectadas: VMware ESXi desde la versión 5.1 hasta la 8.0 (incluyendo más de 155 builds compatibles).

Impacto potencial:

- Escape del Sandbox: Un atacante puede "saltar" desde una máquina virtual aislada hacia el hipervisor subyacente.
- Control total del hipervisor: Una vez en el host, los atacantes pueden manipular, suspender o robar datos de todas las máquinas virtuales que residen en ese servidor físico.
- Bypass de monitoreo: El uso del protocolo VSOCK para comunicación maliciosa permite evadir las herramientas de monitoreo de red tradicionales.
- Persistencia y Ransomware: Esta técnica suele ser el paso previo al despliegue masivo de ransomware en infraestructuras críticas de centros de datos.

Recomendaciones de mitigación:

1. Actualización urgente: Aplicar los parches oficiales de VMware para ESXi de forma prioritaria en todas las instancias afectadas.
2. Detección de procesos VSOCK: Monitorear el uso inusual de sockets virtuales y auditar el sistema mediante el comando lsof -a en hosts ESXi para identificar backdoors activos.
3. Seguridad de Controladores: Restringir la carga de controladores (drivers) no firmados y monitorear modificaciones en los binarios del sistema operativo del host.
4. Fortalecimiento perimetral: Asegurar que las puertas de enlace (VPN y Firewalls) estén actualizadas, ya que son el vector de entrada común para el acceso administrativo inicial.

Prioridad: Crítica.

Ampliar información:

- https://thehackernews.com/2026/01/chinese-linked-hackers-exploit-vmware.html
- https://www.bleepingcomputer.com/news/security/vmware-esxi-zero-days-likely-exploited-a-year-before-disclosure/
- https://csirt.telconet.net/comunicacion/boletines-servicios/explotacion-activa-de-vulnerabilidades-zero-day-en-vmware-esxi-mediante-toolkit-maestro/

MALWARE

BOTNET GOBRUTEFORCER (GOBRUT) — AMENAZA MODULAR EN LINUX DIRIGIDA A ACTIVOS DE CRIPTOMONEDAS

Una variante evolucionada de la botnet basada en Golang está barriendo internet, comprometiendo servidores Linux y bases de datos mediante fuerza bruta inteligente. Esta campaña destaca por su capacidad de evasión y por aprovechar configuraciones predeterminadas sugeridas por Inteligencia Artificial para infiltrarse en sistemas que ejecutan servicios como FTP, MySQL y PostgreSQL.

Resumen técnico:

- Tipo de amenaza: Botnet modular de alta persistencia.
- Lenguaje y ofuscación: Reescrita completamente en Go (Golang) y ofuscada con la herramienta Garbler para dificultar el análisis de seguridad.
- Técnicas de evasión: Implementa enmascaramiento de procesos cambiando su nombre a init o systemd y sobrescribiendo sus argumentos de línea de comandos para ocultarse en los administradores de tareas (ps o top).
- Vector de ataque: Escaneo agresivo de servicios expuestos y fuerza bruta dirigida a credenciales débiles (específicamente nombres de usuario estándar sugeridos por IAs como appuser, myuser u operator).
- Inteligencia de red: Incluye una lista negra de bloques IP del Departamento de Defensa de EE.UU. y proveedores de nube (AWS) para evitar ser detectada por honeypots o equipos de respuesta ante abusos.
- Sistemas en la mira: Servidores Linux con puertos 21 (FTP), 3306 (MySQL), 5432 (PostgreSQL) y paneles de phpMyAdmin.

Impacto potencial:

- Robo de Criptoactivos: Inclusión de módulos para escanear y realizar el "barrido" automático de fondos en billeteras de las redes TRON (TRX) y Binance Smart Chain (BSC). Se han identificado miles de direcciones comprometidas.
- Secuestro de infraestructura: Uso de los servidores infectados para lanzar ataques de denegación de servicio (DDoS) o expandir la red de fuerza bruta a nivel global.
- Compromiso de Datos: Acceso no autorizado a bases de datos críticas, permitiendo la exfiltración de información sensible o la manipulación de registros de negocio.
- Persistencia sigilosa: Capacidad de operar desde directorios temporales simulando procesos críticos del sistema operativo, lo que complica su eliminación manual.

Recomendaciones de mitigación:

1. Fortalecimiento de Credenciales: Eliminar cualquier usuario por defecto y cambiar contraseñas sugeridas por tutoriales o asistentes de IA. Implementar políticas de contraseñas complejas y únicas.
2. Cierre de Puertos y Servicios: No exponer servicios de base de datos o FTP directamente a internet. Utilizar túneles VPN o redes privadas para la administración.
3. Auditoría de Configuraciones IA: Revisar meticulosamente cualquier "receta" o fragmento de código generado por LLMs antes de implementarlo en producción para asegurar que no contenga valores débiles.
4. Monitoreo de Procesos: Vigilar procesos del sistema (init, systemd) que se ejecuten desde rutas inusuales (ej. /tmp o directorios de usuario) y auditar logs de acceso fallidos en servicios de red.
5. Uso de MFA: Habilitar la autenticación multifactor siempre que el servicio lo permita para mitigar el éxito de los ataques de fuerza bruta.

Prioridad: Importante.

Ampliar información:

- https://blog.segu-info.com.ar/2026/01/gobruteforcer-botnet-para-linux-basada.html
- https://unaaldia.hispasec.com/2026/01/gobruteforcer-el-botnet-que-ataca-servidores-linux-de-criptomonedas-con-contrasenas-debiles.html
- https://devel.group/blog/gobruteforcer-recargado-la-botnet-regresa-en-2026-mas-letal-y-con-objetivos-criptograficos/

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

MICROSOFT ALERTA SOBRE CAMPAÑAS DE PHISHING INTERNO POR MALA CONFIGURACIÓN DE ENRUTAMIENTO DE CORREO

Microsoft ha emitido una advertencia crítica sobre un aumento en ataques de phishing que explotan configuraciones de enrutamiento de correo electrónico complejas para suplantar dominios internos de las organizaciones. Paralelamente, la compañía ha liderado una operación internacional para desarticular "RedVDS", una red global que facilitaba este tipo de infraestructuras para estafas digitales a escala masiva.

Resumen técnico:

- Vector de ataque: Los atacantes aprovechan escenarios donde el registro MX (Mail Exchanger) de una organización apunta a un servidor local o a un servicio de filtrado de terceros antes de llegar a Microsoft 365. Esta "brecha" en el flujo de correo permite inyectar mensajes falsificados que el sistema receptor identifica erróneamente como internos.
- Plataformas involucradas: Se ha detectado un uso intensivo del kit de phishing Tycoon 2FA, diseñado para eludir la autenticación multifactor (MFA) mediante técnicas de adversario en el medio (AiTM).
- Temas recurrentes: Los correos fraudulentos suelen suplantar al departamento de Recursos Humanos (RR.HH.), notificaciones de buzón de voz, documentos compartidos de DocuSign o alertas de restablecimiento de contraseñas.

Impacto potencial:

- Operación RedVDS: Microsoft, junto con el FBI y Europol, desmanteló RedVDS, un servicio de suscripción de bajo costo ($24 USD al mes) que proporcionaba infraestructura para este tipo de fraudes.
- Pérdidas económicas: Solo en Estados Unidos, se estima que esta infraestructura facilitó fraudes por más de 40 millones de dólares. Entre las víctimas se encuentran farmacéuticas y asociaciones inmobiliarias que sufrieron desvío de pagos bancarios.
- Uso de IA: La red desmantelada empleaba herramientas de inteligencia artificial para generar conversaciones de correo realistas, clonación de voz y manipulación de video (deepfakes) para engañar a los empleados.

Recomendaciones para mitigar el riesgo:

1. Políticas de autenticación: Establecer políticas estrictas de DMARC con configuración de rechazo (reject) y SPF con fallo estricto (hard fail).
2. Configuración del MX: Microsoft recomienda, siempre que sea posible, apuntar los registros MX directamente a Office 365 para cerrar este vector de exposición.
3. Desactivar Direct Send: Deshabilitar la función de envío directo si no es estrictamente necesaria para evitar la recepción de correos suplantados.
4. Verificación de procesos: Implementar protocolos de validación fuera de banda (vía telefónica o canales conocidos) antes de procesar cambios en instrucciones de pago o transferencias bancarias urgentes.
5. Auditoría de conectores: Revisar y configurar correctamente los conectores de terceros (archivado de correo o filtrado de spam) para asegurar que no se omitan las verificaciones de seguridad de Microsoft.

Prioridad: Importante.

Ampliar Información:

- https://www.msn.com/es-mx/dinero/noticias/microsoft-va-contra-el-redvds-la-red-detr%C3%A1s-de-estafas-millonarias/ar-AA1Ucwmb?ocid=finance-verthp-feeds
- https://es.euronews.com/next/2026/01/14/microsoft-tumba-una-red-global-de-phishing-que-dejo-millones-de-euros-en-fraudes
- https://thehackernews.com/2026/01/microsoft-warns-misconfigured-email.html