GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °1026

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

VULNERABILIDADES

FORTINET — BYPASS DE MFA Y EJECUCIÓN REMOTA DE COMANDOS (CVE-2026-22572 / CVE-2026-25836 / CVE-2026-22627)

Fortinet ha publicado parches para múltiples vulnerabilidades críticas que afectan a su ecosistema de gestión y seguridad, incluyendo FortiManager, FortiAnalyzer y FortiWeb. Paralelamente, investigadores de seguridad han alertado sobre una campaña activa que explota dispositivos FortiGate para infiltrarse en redes corporativas y extraer credenciales críticas de Active Directory.

Resumen técnico:

- Identificadores principales: CVE-2026-22572, CVE-2026-25836 y CVE-2026-22627.
- Severidad: Alta (7.4 en la escala CVSSv3).
- Causa raíz: Fallos en la validación de firmas SSO, inyección de comandos en funciones de actualización y desbordamientos de búfer en procesos de red.
- Mecanismo de falla: Los atacantes pueden evadir la autenticación multifactor (MFA) en la interfaz gráfica, ejecutar comandos arbitrarios a través de APIs de gestión o escalar privilegios hasta nivel de root en sistemas Linux.
- Estado de explotación: Explotación activa confirmada en campañas de robo de configuración y persistencia en red.
- Versiones afectadas: FortiManager (v7.4.0 a v7.4.2), FortiAnalyzer, FortiWeb y FortiClientLinux, entre otros productos del catálogo.

Impacto potencial:

- Bypass de controles de acceso: Un atacante puede obtener acceso administrativo a la consola de gestión omitiendo el segundo factor de autenticación.
- Compromiso total del sistema (RCE): La ejecución remota de comandos permite tomar el control de los appliances de seguridad para manipular el tráfico de red.
- Robo de credenciales de servicios: Los atacantes pueden extraer y descifrar contraseñas de cuentas de servicio (LDAP/AD) almacenadas en los archivos de configuración de los firewalls.
- Movimiento lateral profundo: El acceso inicial facilita la implementación de herramientas de gestión remota (RMM) para saltar hacia controladores de dominio y servidores internos.

Recomendaciones de mitigación:

1. Actualización inmediata a versiones parcheadas: Migrar de forma prioritaria a versiones como FortiManager 7.4.3+, FortiWeb 8.0.3+ o sus equivalentes corregidos según el fabricante.
2. Auditoría de usuarios administrativos: Realizar un escaneo manual de las cuentas locales en busca de usuarios sospechosos creados recientemente (especialmente el nombre de cuenta "support").
3. Fortalecimiento de la retención de registros: Configurar una retención de logs de al menos 60 a 90 días en los dispositivos perimetrales para permitir el análisis forense de intrusiones previas.
4. Restricción de la superficie de exposición: Deshabilitar las interfaces de gestión en la red pública y limitar el acceso administrativo exclusivamente a través de redes VPN confiables.

Prioridad: Urgente.

Ampliar información:

- https://thehackernews.com/2026/03/fortigate-devices-exploited-to-breach.html
- https://www.fortiguard.com/psirt
- https://www.heise.de/en/news/Fortinet-closes-brute-force-and-command-injection-flaws-in-FortiWeb-Co-11207266.html
- https://securityaffairs.com/189241/security/attackers-exploit-fortigate-devices-to-access-sensitive-network-information.html
- https://op-c.net/blog/critical-fortinet-vulnerabilities-under-active-exploitation/
- https://www.rescana.com/post/fortigate-forticloud-sso-authentication-bypass-active-exploitation-of-cve-2025-59718-59719-for-cred

N8N — REMOTE CODE EXECUTION CRÍTICO (CVE-2026-27577 / CVE-2025-68613)

Se han revelado múltiples vulnerabilidades críticas en la plataforma de automatización de flujos de trabajo n8n, incluyendo fallos de escape de sandbox y ejecución remota de código (RCE). Adicionalmente, la agencia CISA ha incluido formalmente el identificador CVE-2025-68613 en su catálogo de vulnerabilidades explotadas conocidas el 11 de marzo de 2026, confirmando que estos fallos están siendo utilizados activamente por actores de amenazas en entornos productivos.

Resumen técnico:

- Identificadores principales: CVE-2026-27577, CVE-2026-27493, CVE-2026-27495, CVE-2026-27497 y CVE-2025-68613.
- Severidad: Crítica (Puntajes CVSS v3.1 de 9.4 a 9.8).
- Causa raíz: Control inadecuado de recursos de código gestionados dinámicamente y fallos de validación en el compilador de expresiones de la plataforma.
- Mecanismo de falla: Usuarios autenticados con permisos de creación de flujos pueden evadir el sandbox para invocar módulos nativos (como child_process) y ejecutar comandos de sistema. Un atacante no autenticado puede encadenar fallos en los nodos de formulario ("Form nodes") para lograr la misma ejecución de código mediante la inyección de expresiones en campos públicos.
- Estado de explotación: Explotación activa confirmada para la serie de fallos de RCE; existen más de 40,000 instancias expuestas a nivel global.
- Versiones afectadas: Versiones autohospedadas y en la nube inferiores a 1.123.22, así como las ramas 2.x inferiores a 2.9.3 y 2.10.1.

Impacto potencial:

- Compromiso total de la instancia: Un atacante puede ejecutar scripts arbitrarios con los privilegios del proceso n8n, tomando el control completo del servidor o contenedor.
- Exfiltración de secretos corporativos: Acceso y descifrado de la base de datos de credenciales, lo que expone llaves de AWS, tokens de OAuth, contraseñas de bases de datos y API keys de servicios integrados.
- Movimiento lateral en la infraestructura: Uso del servidor comprometido como punto de salto para atacar otros recursos internos o servicios en la nube a los que n8n tenga acceso legítimo.
- Manipulación de flujos de trabajo: Alteración de procesos de automatización existentes para interceptar datos sensibles en tránsito o desviar flujos de información hacia infraestructura controlada por el atacante.

Recomendaciones de mitigación:

1. Actualización inmediata: Migrar de forma prioritaria a las versiones parcheadas 2.10.1, 2.9.3 o 1.123.22 para cerrar los vectores de escape de sandbox conocidos.
2. Rotación exhaustiva de credenciales: Cambiar todos los secretos y llaves de acceso almacenados en n8n tras la actualización, asumiendo que pudieron ser comprometidos mediante el acceso a la N8N_ENCRYPTION_KEY.
3. Restricción de permisos de autoría: Limitar estrictamente los permisos para crear o modificar workflows únicamente a personal de total confianza, aplicando el principio de mínimo privilegio.
4. Hardening del entorno de ejecución: Ejecutar n8n en modo de corredor externo (N8N_RUNNERS_MODE=external) y en entornos aislados con red restringida para mitigar el radio de impacto de una posible explotación.

Prioridad: Crítica.

Ampliar información:

- https://thehackernews.com/2026/03/critical-n8n-flaws-allow-remote-code.html
- https://github.com/n8n-io/n8n/security/advisories/GHSA-vpcf-gvg4-6qwr
- https://github.com/n8n-io/n8n/security/advisories/GHSA-75g8-rv7v-32f7
- https://www.bleepingcomputer.com/news/security/cisa-orders-feds-to-patch-n8n-rce-flaw-exploited-in-attacks/
- https://windowsforum.com/threads/cisa-kev-adds-cve-2025-68613-in-n8n-urgent-rce-patch-guide.404752/

SAP — INYECCIÓN DE CÓDIGO Y DESERIALIZACIÓN CRÍTICA EN FS-QUO Y NETWEAVER (CVE-2019-17571 / CVE-2026-27685)

SAP ha publicado 15 notas de seguridad como parte de su ciclo de parches de marzo de 2026, destacando dos vulnerabilidades críticas en los componentes FS-QUO (Quotation Management Insurance) y NetWeaver Enterprise Portal Administration. Estos fallos permiten a atacantes remotos ejecutar código arbitrario, comprometiendo la integridad de entornos empresariales críticos dedicados a la gestión de seguros y servicios financieros.

Resumen técnico:

- Identificadores principales: CVE-2019-17571 y CVE-2026-27685.
- Severidad: Crítica (Puntajes CVSS de 9.8 y 9.1, respectivamente).
- Causa raíz: Uso de una biblioteca obsoleta (Apache Log4j 1.2.17) en el módulo de planificación de FS-QUO y falta de validación de entrada durante la deserialización de objetos Java en NetWeaver.
- Mecanismo de falla: En FS-QUO, un atacante no autenticado puede enviar objetos serializados maliciosos al servicio SocketServer de Log4j para ejecutar comandos remotos. En NetWeaver, un atacante con altos privilegios puede inyectar contenido no confiable que, al ser deserializado, otorga control sobre el portal.
- Estado de explotación: No se han reportado ataques activos específicamente dirigidos a SAP FS-QUO, pero existen exploits públicos (PoC) para la vulnerabilidad de Log4j 1.2 desde 2019.
- Versiones afectadas: SAP FS-QUO versión 800 (módulo scheduler) y SAP NetWeaver EP-RUNTIME versión 7.50.

Impacto potencial:

- Ejecución Remota de Código (RCE): Capacidad para ejecutar comandos arbitrarios en el servidor SAP sin necesidad de autenticación previa en el caso de FS-QUO.
- Compromiso de flujos de negocio: El control sobre el módulo de planificación puede derivar en la manipulación de procesos automatizados de cotización y suscripción de seguros.
- Escalada de privilegios y persistencia: Los atacantes pueden realizar movimientos laterales en la infraestructura del portal y comprometer servicios de identidad vinculados.
- Interrupción de servicios críticos (DoS): Posibilidad de provocar condiciones de denegación de servicio o comprometer la confidencialidad de datos corporativos sensibles.

Recomendaciones de mitigación:

1. Aplicación inmediata de Notas de Seguridad: Implementar la Nota SAP 3698553 para FS-QUO y la Nota SAP 3714585 para NetWeaver de forma prioritaria (idealmente en menos de 24 horas).
2. Actualización o eliminación de Log4j: Seguir las directrices de SAP para eliminar los componentes vulnerables de Log4j 1.2 del módulo scheduler o aplicar el parche de emergencia provisto.
3. Restricción de acceso de red: Limitar el acceso a los puertos de gestión y a los hosts del planificador únicamente a redes internas confiables o mediante túneles VPN.
4. Implementación de MFA: Exigir autenticación multifactor para todos los administradores del portal NetWeaver y monitorear logs en busca de errores de deserialización o conexiones salientes inusuales.

Prioridad: Crítica.

Ampliar información:

- https://erp.today/sap-security-patch-day-march-2026/
- https://www.rescana.com/post/critical-sap-fs-quo-and-netweaver-vulnerabilities-exposed-in-march-2026-security-patch-day-immediat
- https://www.securityweek.com/sap-patches-critical-fs-quo-netweaver-vulnerabilities/amp/
- https://thehackernews.com/2026/03/dozens-of-vendors-patch-security-flaws.html

QUALCOMM — DESBORDAMIENTO DE ENTEROS EN COMPONENTE DE GRÁFICOS (CVE-2026-21385)

Google y Qualcomm han confirmado la existencia de una vulnerabilidad de alta severidad que afecta a más de 235 conjuntos de chips (chipsets) utilizados en una amplia gama de dispositivos Android. El fallo está siendo explotado de forma limitada y dirigida en el mundo real, lo que ha llevado a la agencia CISA a incluirlo en su catálogo de vulnerabilidades explotadas conocidas (KEV), estableciendo un plazo de remediación urgente para organizaciones gubernamentales y corporativas.

Resumen técnico:

- Identificador principal: CVE-2026-21385.
- Severidad: Alta (7.8 en la escala CVSSv3).
- Causa raíz: Desbordamiento o ciclo de enteros (Integer Overflow) en el subcomponente de gráficos y pantalla de Qualcomm.
- Mecanismo de falla: Un atacante local o mediante una aplicación maliciosa puede procesar datos de usuario diseñados específicamente para provocar una corrupción de memoria en capas bajas del hardware (kernel/drivers).
- Estado de explotación: Explotación activa confirmada en ataques dirigidos; el fallo permite evadir defensas tradicionales a nivel de aplicación (sandbox de Android).
- Versiones afectadas: Dispositivos Android con procesadores Qualcomm que no hayan aplicado el nivel de parche de seguridad de marzo de 2026.

Impacto potencial:

- Corrupción de memoria persistente: La explotación exitosa degrada la integridad de la memoria del sistema, permitiendo la inestabilidad o el control de procesos críticos.
- Evasión de controles de seguridad: Al residir en componentes de hardware de bajo nivel, el ataque puede omitir las restricciones impuestas por el sistema operativo y las aplicaciones de seguridad.
- Ejecución de código arbitrario: Permite a un atacante ejecutar instrucciones con privilegios elevados, facilitando el acceso no autorizado a datos sensibles del dispositivo.
- Compromiso total del endpoint: El control del subcomponente de gráficos puede escalar hasta la toma de control del sistema, permitiendo el despliegue de spyware o herramientas de vigilancia.

Recomendaciones de mitigación:

1. Actualización del parche de seguridad: Instalar de manera inmediata el nivel de parche de seguridad de Android 2026-03-05 o superior, el cual contiene las correcciones específicas para los controladores de Qualcomm.
2. Inventario de hardware afectado: Realizar un censo de los modelos de dispositivos y conjuntos de chips Qualcomm en uso dentro de la organización para priorizar la actualización en usuarios de alto riesgo.
3. Monitoreo de comportamiento del endpoint: Utilizar soluciones de defensa contra amenazas móviles (MTD) para detectar anomalías en el comportamiento del hardware y procesos del sistema que sugieran intentos de explotación.
4. Validación de actualizaciones de OEM: Coordinar con los fabricantes de dispositivos (Samsung, Google, Xiaomi, etc.) la disponibilidad de las actualizaciones, dado que los tiempos de implementación varían según el proveedor y el operador.

Prioridad: Crítica.

Ampliar información:

- https://cloud.google.com/blog/topics/threat-intelligence/2025-zero-day-review
- https://www.forbes.com/sites/daveywinder/2026/03/04/critical-android-update-google-confirms-0day-security-bypass-attacks/
- https://zimperium.com/blog/mobile-threat-watch/qualcomm-zero-day-exploited-in-targeted-android-attacks
- https://socprime.com/es/blog/cve-2026-21386-vulnerabilidad/
- https://thehackernews.com/2026/03/weekly-recap-qualcomm-0-day-ios-exploit.html

MALWARE

KADNAP — BOTNET DE DISPOSITIVOS EDGE Y RED DE PROXIES RESILIENTE

Investigadores de Black Lotus Labs han desmantelado el anonimato de una botnet denominada KadNap, que ha comprometido más de 14,000 dispositivos de red, principalmente routers Asus en Estados Unidos. Esta red utiliza un sofisticado diseño peer-to-peer (P2P) para ocultar sus servidores de comando y control (C2), convirtiendo los equipos infectados en una red de proxies residenciales comercializada bajo el nombre "Doppelgänger" para facilitar actividades de cibercrimen de forma anónima.

Resumen técnico:

- Identificador: KadNap Malware (asociado a botnets de proxies "Doppelgänger").
- Severidad: Alta (Debido a su persistencia avanzada y arquitectura descentralizada).
- Causa raíz: Explotación de vulnerabilidades conocidas y no parcheadas en el firmware de routers y dispositivos edge.
- Mecanismo de falla: El compromiso se inicia con un script de shell (aic.sh) que establece persistencia mediante una tarea programada (cron job) que se ejecuta cada 55 minutos. El malware utiliza una versión personalizada del protocolo Kademlia DHT (Distributed Hash Table) para localizar sus servidores de control sin exponer direcciones IP estáticas.
- Estado de explotación: Activa y en crecimiento; se estima un promedio de 14,000 dispositivos infectados diariamente con una alta concentración en EE. UU. (60%).
- Versiones afectadas: Principalmente routers Asus, aunque tiene capacidad de infectar diversos dispositivos con arquitecturas ARM y MIPS.

Impacto potencial:

- Uso no autorizado de ancho de banda: Los dispositivos infectados actúan como nodos de salida para tráfico ajeno, lo que degrada significativamente la velocidad y calidad de la conexión para el usuario legítimo.
- Riesgo reputacional y bloqueos: Al ser utilizada como proxy para cibercrimen, la dirección IP del dispositivo queda asociada a ataques de fuerza bruta o phishing, provocando el bloqueo de la IP en servicios y plataformas web legítimas.
- Persistencia resistente a reinicios: A diferencia de otros malwares de routers, KadNap almacena scripts que se ejecutan automáticamente al reiniciar el equipo, garantizando que el dispositivo sea re-infectado inmediatamente después de un simple apagado/encendido.
- Control administrativo del dispositivo: Los atacantes ganan la capacidad de manipular reglas de firewall internos, cerrar puertos críticos (como el puerto 22 SSH) y utilizar el dispositivo como punto de entrada a la red local.

Recomendaciones de mitigación:

1. Reinicio de fábrica (Factory Reset): Esta es la única medida definitiva para eliminar los scripts de persistencia y archivos binarios maliciosos; un reinicio estándar del dispositivo no es suficiente para la desinfección.
2. Actualización obligatoria de firmware: Validar e instalar las últimas versiones de seguridad proporcionadas por el fabricante para cerrar los agujeros de seguridad que el malware utiliza para su propagación.
3. Fortalecimiento de credenciales: Cambiar inmediatamente las contraseñas de administración por defecto y utilizar claves complejas para evitar ataques de fuerza bruta dirigidos a la interfaz de gestión.
4. Desactivación de administración WAN: Deshabilitar cualquier interfaz de administración o acceso remoto que esté expuesto directamente a Internet, limitando el acceso solo a redes locales de confianza.

Prioridad: Urgente.

Ampliar información:

- https://www.bleepingcomputer.com/news/security/new-kadnap-botnet-hijacks-asus-routers-to-fuel-cybercrime-proxy-network/
- https://www.techradar.com/pro/security/asus-routers-hijacked-to-power-dangerous-cybercrime-proxy-network-heres-what-we-know
- https://securityaffairs.com/189251/malware/kadnap-bot-compromises-14000-devices-to-route-malicious-traffic.html
- https://thehackernews.com/2026/03/kadnap-malware-infects-14000-edge.html
- https://arstechnica.com/security/2026/03/14000-routers-are-infected-by-malware-thats-highly-resistant-to-takedowns/

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 CORRIGE 84 VULNERABILIDADES EN EL PATCH TUESDAY DE MARZO — ALERTAS EN SQL SERVER Y .NET

Microsoft ha desplegado su boletín de seguridad de marzo de 2026, abordando un total de 84 vulnerabilidades nuevas, de las cuales 8 han sido clasificadas como Críticas. La actualización destaca por la inclusión de dos "Zero-Days" de conocimiento público antes del parche, afectando a Microsoft SQL Server y la plataforma .NET, lo que reduce significativamente la ventana de respuesta para las organizaciones.

Resumen técnico:

- Vulnerabilidades totales: 84 fallos parcheados (8 Críticos, 76 Importantes), sumados a 10 actualizaciones de terceros/Chromium.
- Falla destacada en SQL Server (CVE-2026-21262): Vulnerabilidad de elevación de privilegios con puntaje CVSS de 8.8. Permite a un usuario autenticado escalar sus permisos hasta convertirse en administrador del sistema (sysadmin) de forma silenciosa.
- Falla en .NET (CVE-2026-26127): Vulnerabilidad de denegación de servicio (DoS) de conocimiento público que afecta a .NET 9.0 y 10.0, permitiendo ataques remotos no autenticados para desestabilizar aplicaciones.
- Escalación de privilegios: El 55% de los errores corregidos este mes están relacionados con la elevación de privilegios, afectando componentes del kernel de Windows, Winlogon y SMB Server.
- IA y Copilot: Se corrigió el fallo CVE-2026-26144 en Excel, donde un atacante podría engañar a un "Copilot Agent" para extraer datos confidenciales mediante ataques sin clic (Zero-click).
- Cambio en Autopatch: Microsoft ha habilitado por defecto la función de "Hotpatching", que permite aplicar actualizaciones de seguridad críticas sin necesidad de reiniciar los dispositivos.

Impacto potencial:

- Control total de bases de datos: La explotación del fallo en SQL Server permite el robo, modificación o borrado de propiedad intelectual y datos financieros sensibles.
- Interrupción de servicios críticos: Ataques de denegación de servicio en la infraestructura .NET pueden paralizar APIs web, servicios de pago y aplicaciones de línea de negocio.
- Fuga de datos asistida por IA: El uso de agentes de IA (Copilot) en entornos corporativos introduce nuevos vectores donde la información confidencial de Excel puede ser exfiltrada involuntariamente.
- Compromiso total del sistema: Los fallos de ejecución remota de código (RCE) en componentes como Print Spooler y Office permiten a atacantes tomar el control de estaciones de trabajo mediante documentos maliciosos.

Recomendaciones para mitigar el riesgo:

1. Priorización de parches críticos: Aplicar de forma inmediata las actualizaciones para SQL Server (CVE-2026-21262) y .NET, especialmente en servidores con exposición a redes no confiables.
2. Adopción de Windows Autopatch: Configurar la actualización automática con "Hotpatch" para reducir el tiempo de exposición a vulnerabilidades de escalación de privilegios sin interrumpir la operación.
3. Auditoría de privilegios en bases de datos: Revisar y limitar las cuentas de usuario con capacidad de ejecución de consultas en SQL Server para mitigar el riesgo de movimientos laterales.
4. Configuración de seguridad en Agentes de IA: Revisar los permisos y las políticas de acceso a datos de los agentes de Copilot para prevenir la extracción de información mediante inyecciones de comandos en hojas de cálculo.

Prioridad: Crítica.

Ampliar Información:

- https://thehackernews.com/2026/03/microsoft-patches-84-flaws-in-march.html
- https://ciberblog.net/noticias/microsoft-patch-tuesday-marzo-2026-zero-days
- https://cyberdefensa.mx/microsoft-corrige-84-fallas-el-martes-de-parches-de-marzo-incluidos-dos-dias-cero-publicos/
- https://www.ciberplaneta.org/herramientas/microsoft-corrige-84-defectos-en-el-parche-del-martes-de-marzo-incluidos-dos-dias-cero-publicos/
- https://enigmasecurity.cl/zeroday-206/