GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º3625

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	1	0	0

VULNERABILIDADES

VULNERABILIDAD 0-DAY EN WHATSAPP PARA iOS Y macOS (CVE-2025-55177)

El 30 de agosto de 2025, WhatsApp liberó una actualización de emergencia para sus aplicaciones en iOS y macOS, corrigiendo una vulnerabilidad crítica de autorización insuficiente en los mensajes de sincronización de dispositivos vinculados. La falla, identificada como CVE-2025-55177 (CVSS 8.0), habría sido explotada en combinación con la vulnerabilidad CVE-2025-43300 de Apple (ImageIO) en ataques de tipo zero-click dirigidos contra usuarios específicos.

Recursos afectados:

- WhatsApp para iOS (versiones anteriores a 2.25.21.73).
- WhatsApp Business para iOS (versión 2.25.21.78 y anteriores).
- WhatsApp para Mac (versión 2.25.21.78 y anteriores).

Resumen técnico:

- CVE-2025-55177: Autorización insuficiente en la sincronización de dispositivos vinculados.
- Impacto: Un atacante no relacionado podía forzar el procesamiento de contenido desde una URL arbitraria en el dispositivo víctima.
- Explotación: Confirmada en ataques zero-click que no requieren interacción del usuario.
- Cadena de ataque: Potencialmente combinada con CVE-2025-43300 (Apple ImageIO – escritura fuera de límites).

Impacto potencial:

- Ejecución de código remoto en dispositivos Apple mediante campañas de spyware avanzado.
- Compromiso de la privacidad y comunicaciones de objetivos de alto perfil, incluyendo periodistas y defensores de derechos humanos.
- Riesgo de persistencia y espionaje mediante explotación encadenada de múltiples vulnerabilidades.

Recomendaciones de mitigación:

1. Actualizar inmediatamente WhatsApp a las versiones corregidas en iOS y macOS.
2. Restablecer los dispositivos a valores de fábrica si se sospecha compromiso.
3. Mantener actualizado el sistema operativo y las aplicaciones críticas de mensajería.
4. Monitorizar dispositivos móviles de alto riesgo ante posibles indicadores de spyware.

Prioridad: Crítica.

Ampliar Información:

- https://thehackernews.com/2025/08/whatsapp-patches-zero-click-exploit.html
- https://support.apple.com/en-us/124925

- https://ciberseguridad.euskadi.eus/noticia/2025/vulnerabilidad-0-day-explotada-en-varios-productos-de-apple-en-ataques-dirigidos/webcyb00-contcibglos/es/

VULNERABILIDAD "HYDROPH0BIA" EN SECURE BOOT (CVE-2025-4275)

El 1 de septiembre de 2025, medios especializados retomaron la vulnerabilidad Hydroph0bia (CVE-2025-4275), originalmente publicada en junio 2025, tras la difusión de nuevos análisis técnicos y la disponibilidad de exploits públicos en GitHub. El fallo afecta a firmware InsydeH_2O® UEFI BIOS, ampliamente utilizado en portátiles de fabricantes como Huawei, Dell, Lenovo y otros.

Recursos afectados:

- Dispositivos con firmware InsydeH_2O® UEFI BIOS.
- Modelos confirmados: Huawei Matebook 2023, y múltiples equipos Dell/Lenovo con este firmware.

Resumen técnico:

- CVE-2025-4275: Shadowing de variables NVRAM volátiles con el mismo GUID que las persistentes.
- Impacto: Permite engañar al firmware para ejecutar binarios UEFI no firmados como si fueran válidos.
- Explotación: Requiere privilegios administrativos iniciales para plantar un payload en la partición EFI (ESP) y modificar variables NVRAM.
- Resultado: El firmware carga código no firmado durante el arranque, evadiendo Secure Boot.

Impacto potencial:

- Ejecución de bootkits/rootkits con persistencia profunda a nivel pre-OS.
- El malware sobrevive a reinstalaciones del sistema operativo, reemplazo de disco y actualizaciones de firmware.

- Compromiso total de la cadena de arranque segura, con riesgo elevado en entornos críticos.

Recomendaciones de mitigación:

1. Actualizar inmediatamente el firmware BIOS a las versiones corregidas por cada fabricante OEM.
2. Restringir privilegios de administrador en equipos de usuario.
3. Monitorizar integridad de la partición EFI con herramientas como CHIPSEC o UEFI Scanner.
4. Validar periódicamente la configuración de Secure Boot.

Prioridad: Crítica

Ampliar Información:

- https://blog.segu-info.com.ar/2025/09/hydroph0bia-cve-2025-4275-otra.html
- https://www.hackplayers.com/2025/06/hydroph0bia-cve-2025-4275-otro-golpe.html
- https://coderush.me/hydroph0bia-part1/
- https://coderush.me/hydroph0bia-part2/

VULNERABILIDAD CRÍTICA EN FREEPBX (CVE-2025-57819) – EXPLOTACIÓN ACTIVA

El 28 de agosto de 2025 se publicó la vulnerabilidad crítica CVE-2025-57819 en FreePBX, un sistema de telefonía IP ampliamente utilizado por empresas, call centers y proveedores de servicios de voz. El fallo, ya explotado en ataques en la naturaleza, permite a atacantes remotos no autenticados obtener acceso al panel de administración y ejecutar código arbitrario en los servidores afectados. La vulnerabilidad fue calificada con CVSS 10.0 (máxima severidad).

Recursos afectados:

- FreePBX 15 versiones anteriores a 15.0.66.
- FreePBX 16 versiones anteriores a 16.0.89.
- FreePBX 17 versiones anteriores a 17.0.3.

Resumen técnico:

- **CVE-2025-57819 –** combinación de bypass de autenticación (CWE-288) y inyección SQL (CWE-89) en el módulo comercial endpoint.
- Impacto: Acceso no autenticado al panel de administración (ACP), manipulación arbitraria de la base de datos y ejecución remota de código (RCE).
- Vector de ataque: Explotación vía Internet en instancias con el ACP expuesto sin ACLs o filtrado de IPs.
- Explotación activa: Confirmada desde el 21 de agosto de 2025, con creación de backdoors y escalada de privilegios a nivel root.

Impacto potencial:

- Compromiso total de servidores FreePBX con movimiento lateral en redes internas.
- Exposición a ransomware, fraude de llamadas premium y venta de accesos en foros clandestinos.
- Alto riesgo en organizaciones que dependan de FreePBX como infraestructura crítica de comunicaciones.

Recomendaciones de mitigación:

1. Actualizar inmediatamente a FreePBX 15.0.66, 16.0.89 o 17.0.3.
2. Restringir el acceso al panel de administración mediante ACLs, VPNs o filtrado de IP.
3. Auditar entornos para detectar IoCs asociados.
4. Desconectar de Internet y reinstalar sistemas donde se confirme compromiso.

Prioridad: Crítica.

Ampliar Información:

- https://github.com/FreePBX/security-reporting/security/advisories/GHSA-m42g-xg4c-5f3h
- https://community.freepbx.org/t/security-advisory-please-lock-down-your-administrator-access/107203
- https://thehackernews.com/2025/08/freepbx-servers-targeted-by-zero-day.html
- https://www.cve.org/CVERecord?id=CVE-2025-57819

Recomendaciones Generales Sobre Vulnerabilidades:

Para mitigar las vulnerabilidades en los sistemas, se recomiendan las siguientes medidas claves.

1. Aplicar las actualizaciones de seguridad proporcionadas por Microsoft para las versiones afectadas de Windows Server
2. Instalar regularmente parches de seguridad para corregir vulnerabilidades conocidas.
3. Añadir una capa extra de protección para dificultar el acceso no autorizado por medio de 2FA.
4. Minimizar los permisos de usuarios y aplicaciones para reducir riesgos.
5. Implementar actualizaciones gradualmente, con capacidad de revertir cambios en caso de errores.
6. Usar herramientas de detección de intrusiones para identificar actividades sospechosas.

MALWARE

LAZARUS GROUP AMPLÍA SU ARSENAL (PondRAT, ThemeForestRAT y RemotePE)

El 2 de septiembre de 2025, investigadores de Fox-IT (NCC Group) reportaron que el grupo norcoreano Lazarus desplegó una campaña de ingeniería social contra el sector de finanzas descentralizadas (DeFi). La operación incluyó la distribución de tres RATs (Remote Access Trojans) de nueva generación: PondRAT, ThemeForestRAT y RemotePE, utilizados en diferentes fases de ataque para espionaje y persistencia.

Resumen técnico:

- PondRAT: RAT básico, activo desde al menos 2021, que permite lectura/escritura de archivos, ejecución de procesos y shellcode, con comunicación HTTP(S) hacia un C2.
- ThemeForestRAT: Ejecutado en memoria, con hasta 20 comandos para enumerar archivos, procesos, ejecutar instrucciones, inyectar shellcode, timestomping y monitorizar sesiones RDP. Comparte similitudes con malware usado por Lazarus en el ataque a Sony Pictures (2014).
- RemotePE: RAT avanzado en C++ instalado tras eliminar rastros de fases previas, diseñado para objetivos de alto valor, desplegado mediante loaders específicos (RemotePELoader, DPAPILoader).
- Cadena de ataque: Ingeniería social vía Telegram + sitios falsos (Calendly/Picktime) → PerfhLoader como dropper inicial → despliegue secuencial de PondRAT, ThemeForestRAT y finalmente RemotePE.

Impacto potencial:

- Compromiso completo de redes corporativas en sectores financieros y tecnológicos.
- Recolección de credenciales, cookies de navegadores y datos sensibles mediante keyloggers y stealers.
- Persistencia profunda en sistemas críticos gracias a RATs en memoria y herramientas de proxy/red.
- Posible uso de exploits zero-day (ej. en Chrome) para acceso inicial.
- Riesgo elevado para periodistas, empresas de alto perfil y proyectos DeFi, objetivo habitual de Lazarus.

Recomendaciones de mitigación:

1. Capacitar a usuarios contra campañas de ingeniería social en plataformas de mensajería.
2. Mantener navegadores y aplicaciones actualizadas ante posibles zero-days.

3. Implementar EDR con capacidad de detectar ejecución en memoria, RATs y herramientas como Mimikatz o proxys internos.
4. Monitorear tráfico hacia C2 HTTP(S) sospechosos y uso de loaders como PerfhLoader.
5. Restringir y auditar el uso de cuentas privilegiadas en entornos críticos.

Prioridad: Urgente

Ampliar Información:

- https://thehackernews.com/2025/09/lazarus-group-expands-malware-arsenal.html
- https://blog.segu-info.com.ar/2025/09/lazarus-group-amplia-su-arsenal-de.html
- https://blog.fox-it.com/2025/09/01/three-lazarus-rats-coming-for-your-cheese/

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

INTENTO DE ROBO DE $130M EN FINTECH BRASILEÑA

El 29 de agosto de 2025, atacantes cibernéticos intentaron robar 130 millones de dólares de la empresa brasileña Sinqia S.A., subsidiaria de Evertec Inc., tras comprometer su entorno conectado al sistema de pagos instantáneos Pix del Banco Central de Brasil. El incidente fue reportado oficialmente ante la SEC (Securities and Exchange Commission) de EE.UU.

Resumen técnico:

- Vector de ataque: Uso de credenciales robadas de un proveedor de TI para acceder al entorno Pix de Sinqia.
- Objetivo: Realizar transferencias no autorizadas entre instituciones financieras clientes de Sinqia.
- Detección y respuesta: La compañía detuvo el procesamiento de transacciones en Pix y activó protocolos de respuesta con expertos forenses externos.
- Situación actual: Parte de los fondos ya fueron recuperados, aunque no se ha precisado el monto. El Banco Central revocó temporalmente el acceso de Sinqia a Pix hasta nuevas validaciones.

Impacto potencial:

- Compromiso de la plataforma de pagos más usada en Brasil (Pix), con alto riesgo financiero y reputacional.
- Pérdida de confianza en servicios de fintech e instituciones asociadas (24 entidades financieras dependen del entorno Pix de Sinqia).
- Riesgo de ataques similares mediante supply chain o abuso de credenciales de terceros.

- Explotación recurrente de Pix por malware bancario y campañas dirigidas contra clientes e infraestructura financiera.

Recomendaciones para mitigar el riesgo:

- Implementar autenticación multifactor (MFA) y controles de acceso más estrictos para cuentas de proveedores y terceros.
- Auditar y monitorear accesos privilegiados a entornos críticos de pago.
- Establecer segmentación de redes y limitar el acceso a infraestructuras de alto riesgo como Pix.
- Mantener planes de respuesta y coordinación con autoridades financieras para minimizar impacto en incidentes de fraude.

Prioridad: Crítica.

Ampliar Información:

- https://www.bleepingcomputer.com/news/security/hackers-breach-fintech-firm-in-attempted-130m-bank-heist/