GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °3425

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

VULNERABILIDADES

VULNERABILIDADES CRÍTICAS Y ALTAS EN FORTISIEM, FORTIWEB Y FORTIOS

El PSIRT de Fortinet ha publicado 13 avisos de seguridad que afectan a múltiples dispositivos (FortiSIEM, FortiOS, FortiWeb, FortiProxy, FortiPAM, FortiSOAR, entre otros). Entre ellas destacan varias fallas de ejecución remota de comandos y omisión de autenticación, con exploits disponibles públicamente en algunos casos.

Resumen técnico:

- **CVE-2025-25256 – FortiSIEM (CRÍTICO):** Inyección de comandos no autenticados en CLI [CWE-78]. Permite a un atacante remoto ejecutar código arbitrario sin credenciales válidas. Exploit funcional ya disponible.
- **CVE-2025-52970 – FortiWeb (ALTO):** Omisión de autenticación [CWE-233]. Permite a un atacante remoto acceder como usuario legítimo mediante parámetros manipulados.
- **CVE-2024-26009 – FortiOS / FortiProxy / FortiPAM / FortiSwitchManager (ALTO):** Autenticación débil en protocolo FGFM [CWE-288]. Un atacante que conozca el

número de serie del FortiManager puede tomar control total del dispositivo gestionado.

Impacto potencial:

- Ejecución remota de código y escalada de privilegios.
- Acceso no autorizado a sistemas críticos de seguridad perimetral.
- Riesgo de compromiso total de la red corporativa, incluyendo gestión de firewalls, proxies y sistemas SIEM.
- Posibilidad de explotación inmediata debido a la disponibilidad pública de exploits en algunos casos.

Recomendaciones de mitigación:

1. Aplicar inmediatamente las actualizaciones de seguridad publicadas por Fortinet para cada producto afectado.
2. Deshabilitar o restringir el acceso público a las interfaces de administración de los dispositivos.
3. Revisar logs e indicadores en busca de actividad sospechosa (inicios de sesión no reconocidos, cambios de configuración).
4. Implementar MFA en accesos administrativos y aplicar segmentación de red con ACL estrictas.
5. Deshabilitar servicios o funciones no utilizadas.
6. Verificar la integridad de los dispositivos después de la actualización.

Prioridad: Crítica.

Ampliar Información:

- https://fortiguard.fortinet.com/psirt/FG-IR-25-152
- https://nvd.nist.gov/vuln/detail/CVE-2025-52970
- https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2025-52970
- https://nvd.nist.gov/vuln/detail/CVE-2025-52970
- https://nvd.nist.gov/vuln/detail/CVE-2024-26009
- https://digital.nhs.uk/cyber-alerts/2025/cc-4691

VULNERABILIDAD DE ESCALAMIENTO DE PRIVILEGIOS EN WINDOWS (CLFS) EXPLOTADA POR PIPEMAGIC PARA DESPLEGAR RANSOMEXX

La vulnerabilidad crítica CVE-2025-29824 corresponde a un fallo de escalamiento de privilegios en el subsistema CLFS (Common Log File System) de Windows, esta fue corregida por Microsoft en abril de 2025. Sin embargo, investigadores confirmaron que sigue siendo explotada activamente en agosto de 2025 mediante el troyano PipeMagic, utilizado para desplegar RansomExx.

Se trata de la segunda Zero-Day de Windows aprovechada por este malware en 2025, tras la CVE-2025-24983 en el subsistema Win32k

Resumen técnico:

- CVE-2025-29824 (CLFS, EoP):
- Permite a un atacante elevar privilegios locales hasta SYSTEM.
- Explotada en campañas atribuidas al grupo Storm-2460.
- CVE-2025-24983 (Win32k, EoP): otro Zero-Day explotado por PipeMagic en mayo de 2025.
- Antecedentes: PipeMagic ya fue observado en 2022 desplegando RansomExx y Nokoyawa, explotando también CVE-2023-28252 (CLFS) y la falla de SMB CVE-2017-0144 (EternalBlue) para infiltración inicial.

Impacto potencial:

- Escalada de privilegios hasta SYSTEM, facilitando ejecución de código malicioso y despliegue de ransomware.
- Robo de credenciales (ej. extracción de LSASS con herramientas como ProcDump renombrado).
- Expansión lateral en redes.
- Afectación a sectores TI, financiero, retail, inmobiliario y software en EE.UU., Venezuela, España, Arabia Saudita y Brasil.

Recomendaciones de mitigación:

1. Aplicar los parches de abril–mayo 2025 que corrigen CVE-2025-29824 y CVE-2025-24983 en Windows.
2. Deshabilitar SMBv1 y aplicar actualizaciones completas para mitigar CVE-2017-0144.
3. Restringir el uso de MSBuild en equipos no desarrolladores (AppLocker / WDAC).
4. Monitorizar tuberías nombradas sospechosas (\\\\.\\pipe\\1.<hex>), cargas laterales de googleupdate.dll y ejecución anómala de dllhost.exe accediendo a LSASS.

Prioridad: Critica.

Ampliar Información:

- https://blog.segu-info.com.ar/2025/08/pipemagic-troyano-que-explota-una.html
- https://www.kaspersky.com/about/press-releases/the-magical-comeback-kaspersky-and-bizone-report-new-pipemagic-activity-in-saudi-arabia-and-brazil
- https://nvd.nist.gov/vuln/detail/CVE-2025-29824
- https://unaaldia.hispasec.com/2025/04/pipemagic-explotacion-de-cve-2025-29824-en-clfs-vinculada-a-campanas-de-ransomware.html
- https://securelist.com/pipemagic/117270/

VULNERABILIDADES CRÍTICAS EN SAP NETWEAVER CON EXPLOIT PÚBLICO

Investigadores de Onapsis confirmaron la existencia de un exploit público que combina dos vulnerabilidades críticas en SAP NetWeaver Visual Composer, permitiendo a atacantes no autenticados eludir la autenticación y ejecutar código remoto con privilegios elevados. Aunque SAP publicó parches en abril y mayo de 2025, las fallas fueron explotadas como Zero-Day desde marzo y actualmente están siendo utilizadas por grupos de ransomware y espionaje.

Resumen técnico:

- CVE-2025-31324 (CVSS 10.0): Falta de verificación de autorización en Visual Composer.
- CVE-2025-42999 (CVSS 9.1): Deserialización insegura en Visual Composer.
- Cadena de ataque:
  - CVE-2025-31324 permite eludir autenticación y cargar la carga maliciosa.
  - CVE-2025-42999 deserializa y ejecuta la carga con privilegios de administrador SAP.

Impacto adicional:

  - Implantación de web shells.
  - Ejecución de ataques Living off the Land (LotL) sin necesidad de artefactos adicionales.
  - Nuevas vulnerabilidades relacionadas en deserialización (parcheadas en julio 2025): CVE-2025-30012, CVE-2025-42963, CVE-2025-42964, CVE-2025-42966 y CVE-2025-42980.

Impacto potencial:

- Compromiso total de sistemas SAP NetWeaver afectados.
- Acceso no autorizado a datos sensibles y procesos empresariales.
- Uso por grupos de ransomware como Qilin, BianLian y RansomExx, así como equipos de espionaje con vínculos a China.
- Riesgo crítico para organizaciones que operan infraestructura crítica.

Recomendaciones de mitigación:

1. Aplicar inmediatamente los parches de abril, mayo y julio 2025 publicados por SAP.
2. Restringir acceso a Visual Composer y aplicaciones SAP desde Internet.
3. Implementar monitoreo para detectar signos de compromiso, incluyendo creación de web shells o ejecución de comandos inusuales.
4. Revisar integridad de sistemas SAP y aplicar endurecimiento adicional en configuraciones críticas.

5. Utilizar herramientas de análisis y scanners especializados (ej. RedRays Scanner para CVE-2025-31324).

Prioridad: Crítico

Ampliar Información:

- https://nvd.nist.gov/vuln/detail/CVE-2025-31324
- https://www.lavelez.com.ar/technology/nuevo-exploit-para-sap-de-vulnerabilidad-de-0-dias-supuestamente-lanzado-en-la-naturaleza-por-shinyhunters-hackers/194292/
- https://blog.segu-info.com.ar/2025/08/exploit-publico-para-vulnerabilidades.html
- https://www.incibe.es/en/incibe-cert/early-warning/vulnerabilities/cve-2025-31324
- https://support.sap.com/en/my-support/knowledge-base/security-notes-news/may-2025.html

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 Serve
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

PIPEMAGIC UTILIZADO PARA DESPLEGAR RANSOMEXX

Investigadores de Kaspersky y BI.ZONE confirmaron que el troyano PipeMagic sigue activo en 2025, siendo utilizado por el grupo Storm-2460 para desplegar el ransomware RansomExx. Este malware modular funciona como loader y backdoor, aprovechando vulnerabilidades de Windows (CLFS, Win32k) para escalar privilegios y expandirse lateralmente.

Resumen técnico:

- Detectado desde 2022 en ataques de RansomExx y Nokoyawa.
- Implementado mediante archivos MSBuild maliciosos con cargas cifradas.
- Usa un mecanismo único de tuberías nombradas (\\\\.\\pipe\\1.<hex>) para comunicación cifrada.
- Descarga módulos adicionales desde infraestructura en Microsoft Azure.
- Emplea técnicas de evasión: DLL hijacking (ej. googleupdate.dll), falsos clientes de ChatGPT, cargadores disfrazados de archivos de ayuda (metafile.mshi).
- Nuevas versiones (2025) incorporan persistencia mejorada y uso de ProcDump renombrado como dllhost.exe para extraer credenciales de LSASS.

Funciones avanzadas:

- Comunicación mediante tuberías nombradas cifradas para transferir payloads.
- Arquitectura modular: plugins para comunicación asíncrona, carga de payloads en memoria e inyección de ejecutables C#.
- Técnicas de evasión: DLL hijacking (googleupdate.dll falso), clientes falsos de ChatGPT y cargadores disfrazados como archivos de ayuda.

- Persistencia mejorada y movimiento lateral en versiones 2025, con uso de ProcDump renombrado como dllhost.exe para extracción de credenciales.

- Disponibilidad: PipeMagic sigue activo en 2025, con campañas detectadas en Arabia Saudita y Brasil
- El hallazgo de nuevas variantes confirma que los atacantes continúan desarrollando y expandiendo sus capacidades.

Impacto potencial:

- Cifrado y extorsión a gran escala (RansomExx).
- Robo de credenciales y movimiento lateral en entornos corporativos.
- Compromiso de sectores TI, financiero, retail e industrial en EE.UU., Venezuela, España, Arabia Saudita y Brasil.

Recomendaciones de mitigación:

1. Mantener los sistemas Windows completamente actualizados (parches de abril y mayo 2025 que corrigen CVE-2025-29824 y CVE-2025-24983).
2. Deshabilitar SMBv1 y reforzar controles sobre puertos 445/139.
3. Bloquear ejecución de MSBuild en equipos que no requieran desarrollo.
4. Monitorizar creación de tuberías \\\\.\\pipe\\1.<hex>, procesos anómalos de dllhost.exe y cargas laterales sospechosas de DLL.
5. Implementar soluciones EDR/IDS con reglas específicas contra PipeMagic y RansomExx.

Prioridad: Crítica.

Ampliar Información:

- https://blog.segu-info.com.ar/2025/08/pipemagic-troyano-que-explota-una.html
- https://nvd.nist.gov/vuln/detail/CVE-2025-29824
- https://unaaldia.hispasec.com/2025/04/pipemagic-explotacion-de-cve-2025-29824-en-clfs-vinculada-a-campanas-de-ransomware.html

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

FALLOS EN WINDOWS 11 (KB5063878) – POSIBLE PÉRDIDA DE DATOS EN SSD/HDD

El 12 de agosto de 2025 Microsoft lanzo la actualización Windows 11 24H2 – KB5063878. En días posteriores se han reportado fallos graves en ciertos dispositivos de almacenamiento, especialmente en SSDs con controladores Phison NAND y modelos de fabricantes como WD, Corsair, Kioxia, SanDisk y Samsung. Ver listado de

Resumen técnico:

- Los problemas se manifiestan en operaciones de escritura intensiva de 50 GB o más, sobre todo en unidades con más del 60 % de ocupación.
- Los dispositivos pueden volverse no reconocidos por el sistema operativo, con corrupción o pérdida permanente de datos.

- No se trata de un ataque externo, sino de un bug interno del subsistema de caché de escritura de Windows.
- Microsoft aún no ha emitido un comunicado oficial, mientras que Phison confirmó que está investigando los controladores afectados.

Impacto potencial:

- Riesgo de pérdida permanente de información.
- Inaccesibilidad de unidades críticas en entornos productivos.
- Afectación confirmada en modelos como:
  - WD Blue SA510 2TB SATA, Blue SN5000 2TB NVMe, Red SA500 2TB SATA
  - Corsair Force MP600 NVMe, MP510 960GB NVMe
  - Kioxia Exceria Plus G4
  - Phison Controlador PS5012-E12 NVMe
  - SanDisk Extreme PRO M.2 NVMe 3D
  - Samsung 970 Evo y 990 Pro
  - Unidades NVMe con controladores InnoGrit y Maxio.

Recomendaciones:

- Aplazar la aplicación de KB5063878 en sistemas críticos.
- Evitar cargas de escritura intensiva hasta que Microsoft lance un parche seguro de actualización que corrija este fallo.
- Informar a usuarios críticos sobre los síntomas y prevenir tareas riesgosas.
- Reforzar copias de seguridad aplicando la regla 3-2-1.
- Monitorear anuncios oficiales de Microsoft y Phison.
- Revisar proactivamente sobre el inventario de equipos cuales serían los posibles equipos afectados y cuales están próximos a afectarse.
- Si no se puede evitar la actualización, considerar realizar pruebas en entornos aislados, monitorear el comportamiento del almacenamiento, y tener planes claros de recuperación de ser necesario.

- Si ya está aplicado el parche, no se recomienda desinstalar, se recomienda proceder con el respaldo de la información, se desconoce información del resultado posterior a la desinstalación; tener presente que en el respaldo se debe evitar hacer cargas de transferencia masivos locales ya que es un causante reconocido que activa el fallo, como alternativa usar sincronización con nube y hacerlo paulatinamente.

Prioridad: Crítica

Ampliar información:

- https://learn.microsoft.com/en-us/answers/questions/4371042/windows-11-24h2-update-problems-%28from-23h2%29-border?utm_source=chatgpt.com
- https://www.windowscentral.com/microsoft/windows-11/windows-24h2-update-nuking-ssds-what-to-do
- https://www.tomshardware.com/pc-components/ssds/latest-windows-11-security-patch-might-be-breaking-ssds-under-heavy-workloads-users-report-disappearing-drives-following-file-transfers-including-some-that-cannot-be-recovered-after-a-reboot
- https://www.techradar.com/computing/windows/bug-in-windows-11-update-reportedly-breaks-some-ssds-heres-what-you-need-to-know
- https://www.itpro.com/software/windows/a-windows-11-update-bug-is-breaking-ssds-heres-what-you-can-do-to-prevent-it

PHISHING EN GMAIL PERMITE "HACKEAR" LOS RESÚMENES DE IA DE GEMINI.

Google y el grupo de investigación 0din (Mozilla Zero-Day Research) alertaron sobre una nueva técnica de inyección indirecta de indicaciones (IPI) en Gemini for Workspace, integrada en Gmail. El ataque consiste en ocultar instrucciones maliciosas dentro del HTML de un correo (p. ej., con font-size:0 o color:white), invisibles para el usuario, pero procesadas por el modelo de IA.

Resumen técnico:

- Al hacer clic en "Resumir este correo", Gemini interpreta la instrucción oculta y genera una advertencia de phishing falsa como si proviniera de Google.
- El usuario confía en el aviso generado y puede ser inducido a entregar credenciales o caer en fraudes.

- Este tipo de ataques se consideran las “nuevas macros de correo electrónico”, ya que subvierten la lógica de seguridad mediante instrucciones invisibles.

Impacto potencial:

- Riesgo para los 2000 millones de usuarios de Gmail.
- Posible robo de credenciales, ejecución de fraudes o ingeniería social avanzada.
- El ataque puede eludir filtros antispam tradicionales, ya que el texto malicioso no es visible para ellos.

Recomendaciones para mitigar el riesgo:

- Enseñar a los usuarios que los resúmenes de Gemini son informativos, no alertas de seguridad oficiales de Google.
- Implementar filtros de seguridad para detectar correos con etiquetas ocultas o con texto blanco o tamaño cero.
- Desconfiar de advertencias de seguridad presentadas únicamente en resúmenes de IA; Google no emite alertas de esa forma.
- Mantener vigilancia sobre los desarrollos de seguridad en herramientas basadas en IA en correo electrónico y mensajería.

Prioridad: Critica

Ampliar Información:

- https://www.itsitio.com/seguridad/google-advierte-sobre-una-nueva-estafa-invisible-que-engana-a-gmail-para-robar-contrasenas/
- https://blog.segu-info.com.ar/2025/08/phishing-para-de-gmail-permite-hackear.html
- https://support.google.com/a/answer/16479560?hl=es&authuser=4&ref_topic=7556782