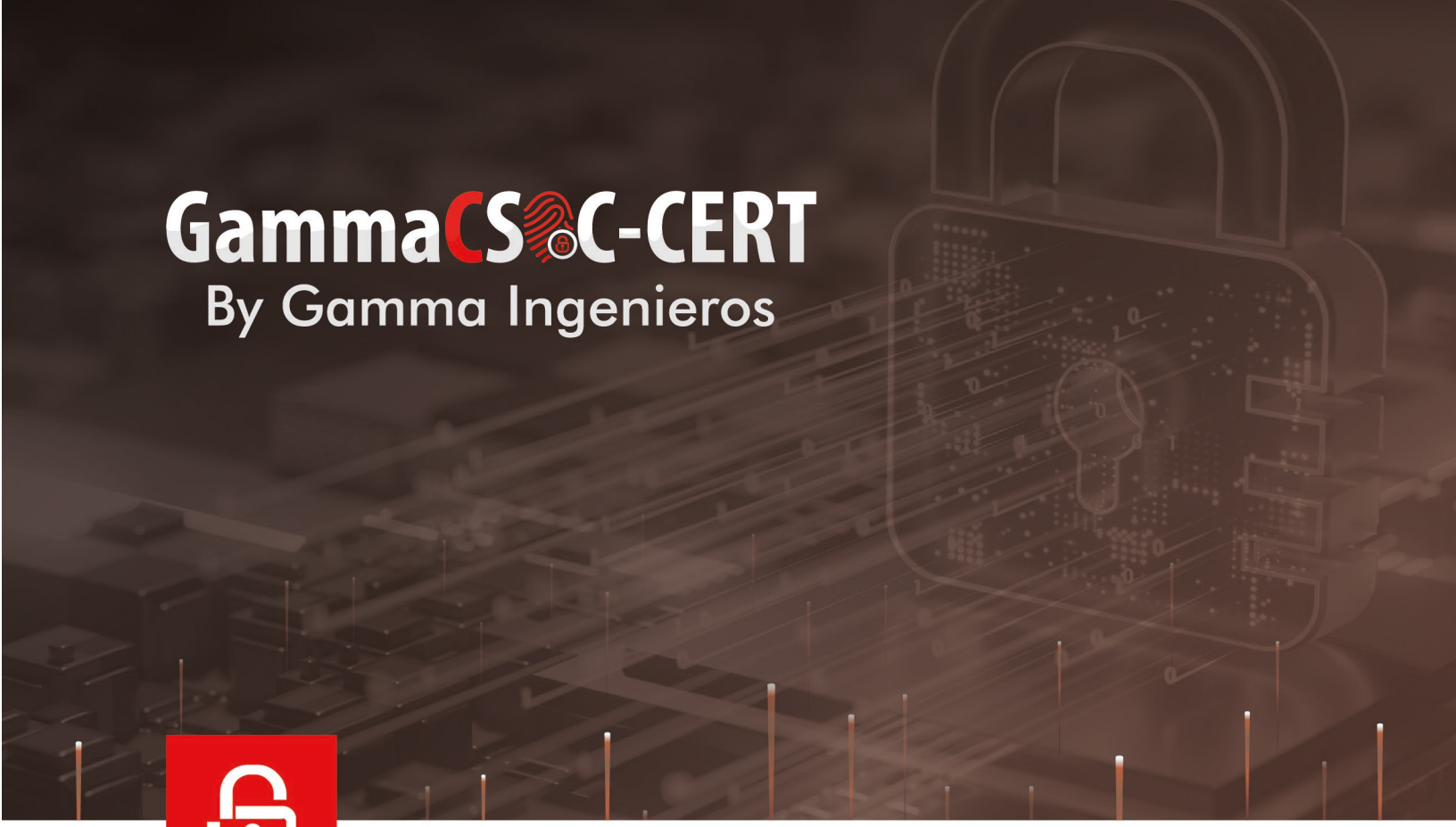
GammaCSOC-CERT
By Gamma Ingenieros



GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º3925

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	1	0

VULNERABILIDADES

VULNERABILIDAD CRÍTICA EN MICROSOFT ENTRA ID – CVE-2025-55241

El 22 de septiembre de 2025, Microsoft divulgó la corrección de una vulnerabilidad crítica en Entra ID (antes Azure Active Directory) que permitía la suplantación de cualquier usuario, incluidos Global Administrators, en cualquier tenant. Identificada como CVE-2025-55241 y con puntaje CVSS 10.0, la falla fue corregida de forma automática el 17 de julio de 2025. No se han reportado casos de explotación activa en entornos productivos.

Resumen técnico:

- CVE-2025-55241 (CVSS 10.0, Privilege Escalation): combinación de dos fallos:
- Uso de Actor tokens emitidos por el Access Control Service (ACS).
- Validación deficiente de tenants en la API heredada Azure AD Graph (graph.windows.net).

- Un atacante podía generar un token en su propio tenant y usarlo para autenticarse como cualquier usuario en otro tenant, sin necesidad de acceso previo.
- Los tokens funcionaban incluso bajo políticas de Conditional Access y carecían de registros en la API legacy, lo que dificultaba la detección de abusos.
- Potencial de impersonación de Global Administrators, lo que habilita creación de cuentas, escalamiento de privilegios, acceso a SharePoint Online, Exchange Online y recursos de Azure vinculados.
- El ataque podía bypassear MFA y dejar pocos rastros en logs, elevando el riesgo de intrusión sigilosa.

Impacto potencial:

- Compromiso total de tenants en Entra ID, incluyendo control administrativo y acceso a servicios críticos en la nube.
- Exfiltración de datos sensibles: información de usuarios, grupos, roles, aplicaciones, dispositivos y claves de BitLocker sincronizadas.
- Riesgo de persistencia a gran escala y movimientos laterales en entornos híbridos (Azure + Microsoft 365).
- Posible abuso en cadenas de suministro y entornos interconectados mediante cuentas guest o integraciones B2B.

Recomendaciones de mitigación:

1. Confirmar que la organización ya recibió la corrección automática aplicada por Microsoft el 17 de julio de 2025.
2. Eliminar dependencias de la API Azure AD Graph, migrando integraciones a Microsoft Graph.
3. Revisar y reducir permisos de aplicaciones y service principals, aplicando principio de mínimo privilegio.
4. Auditar cuentas con rol de Global Administrator y reforzar gobernanza con Privileged Identity Management (PIM).
5. Rotar credenciales y certificados de aplicaciones críticas, especialmente aquellas con permisos delegados amplios.

6. Monitorizar accesos y actividad de tokens sospechosos, así como la creación de cuentas o roles privilegiados inusuales.

Prioridad: Crítica.

Ampliar Información:

- https://thehackernews.com/2025/09/microsoft-patches-critical-entra-id.html
- https://unaaldia.hispasec.com/2025/09/microsoft-soluciona-grave-vulnerabilidad-en-entra-id-que-permitia-suplantar-cualquier-identidad.html
- https://www.bankinfosecurity.com/microsoft-patches-critical-entra-id-flaw-a-29495

VULNERABILIDAD ZERO-DAY EN GOOGLE CHROME – CVE-2025-10585

El 18 de septiembre de 2025, Google lanzó una actualización de seguridad urgente para su navegador Chrome, corrigiendo cuatro vulnerabilidades, entre ellas una zero-day crítica que estaba siendo explotada en la naturaleza. La falla, identificada como CVE-2025-10585, corresponde a un type confusion en el motor V8 JavaScript y WebAssembly.

Resumen técnico:

- CVE-2025-10585 (Zero-Day, V8 Engine): error de type confusion que permite a un atacante remoto inducir comportamientos inesperados, como ejecución de código arbitrario o bloqueos del navegador.
- Descubierta por el Threat Analysis Group (TAG) de Google el 16 de septiembre de 2025.
- Confirmada la existencia de explotación activa en la naturaleza, aunque Google no ha revelado detalles técnicos ni atribución para evitar un abuso masivo.
- Es la sexta vulnerabilidad zero-day de Chrome en 2025 que se confirma bajo explotación activa, junto con CVE-2025-2783, CVE-2025-4664, CVE-2025-5419, CVE-2025-6554 y CVE-2025-6558.
- El vector de ataque más probable consiste en sitios web maliciosos o comprometidos con JavaScript especialmente diseñado.

Impacto potencial:

- Compromiso del sistema del usuario mediante ejecución remota de código al visitar un sitio web manipulado.
- Ampliación del alcance de campañas de cibercrimen: posible uso en exploits kits, ataques dirigidos y distribución de malware.
- Riesgo de afectar a millones de usuarios y organizaciones que dependen de Chrome y navegadores basados en Chromium (Edge, Brave, Opera, Vivaldi).
- Posible encadenamiento con otras vulnerabilidades del navegador o del sistema operativo para alcanzar escalamiento de privilegios.

Recomendaciones de mitigación:

1. Actualizar inmediatamente Chrome a las versiones corregidas: Windows y macOS: 140.0.7339.185/.186 y para Linux: 140.0.7339.185
2. Verificar la instalación: Menú > Ayuda > Información de Google Chrome > Reiniciar navegador.
3. Extender las actualizaciones a navegadores basados en Chromium (Edge, Brave, Opera, Vivaldi) tan pronto como publiquen sus parches.
4. Aplicar políticas de parcheo urgente en entornos corporativos, priorizando equipos con acceso a internet y estaciones de trabajo críticas.
5. Implementar controles adicionales de seguridad perimetral (proxy, sandboxing, bloqueo de sitios maliciosos).
6. Sensibilizar a usuarios sobre riesgos de navegación y phishing mientras se completa el despliegue del parche.

Prioridad: Crítica

Ampliar Información:

- https://thehackernews.com/2025/09/google-patches-chrome-zero-day-cve-2025.html
- https://unaaldia.hispasec.com/2025/09/google-corrige-un-zero-day-critico-en-chrome-cve-2025-10585.html
- https://socprime.com/blog/cve-2025-10585-zero-day-vulnerability/

VULNERABILIDAD CRÍTICA EN FORTRA GOANYWHERE MFT – CVE-2025-10035

El 19 de septiembre de 2025, Fortra publicó un parche de emergencia para GoAnywhere Managed File Transfer (MFT) tras descubrirse una vulnerabilidad crítica de deserialización insegura en el componente License Servlet. Identificada como CVE-2025-10035, la falla tiene una severidad de CVSS 10.0 y puede ser explotada para lograr ejecución remota de comandos (RCE).

Resumen técnico:

- CVE-2025-10035 (CVSS 10.0, CWE-502, CWE-77): el License Servlet acepta respuestas de licencia firmadas de forma inválida.
- Un atacante remoto, con una respuesta de licencia falsificada, puede deserializar objetos maliciosos y ejecutar comandos arbitrarios en el sistema.
- La explotación depende de que la consola de administración esté expuesta a internet, condición común dado el diseño de GoAnywhere.
- Producto afectado: GoAnywhere MFT (todas las versiones previas a 7.8.4 y 7.6.3 Sustain Release).
- Al igual que CVE-2023-0669 (ampliamente explotada en 2023 por actores de ransomware), esta falla se ubica en la misma ruta de código de licenciamiento del Admin Console, lo que incrementa el riesgo de que grupos criminales la aprovechen pronto.

Impacto potencial:

- Ejecución remota de código en servidores MFT vulnerables.
- Robo, alteración o eliminación de datos sensibles transferidos entre socios y clientes.
- Compromiso de integraciones críticas de cadena de suministro y riesgo de ataques de ransomware.
- Posible uso en campañas de explotación masiva, como ocurrió en 2023 con Cl0p y CVE-2023-0669.

Recomendaciones de mitigación:

1. Actualizar inmediatamente a las versiones corregidas: GoAnywhere MFT 7.8.4 y GoAnywhere MFT Sustain Release 7.6.3
2. Si no es posible actualizar de inmediato: Asegurar que la Admin Console no esté expuesta públicamente a internet y Monitorear logs en busca de errores con la cadena SignedObject.getObject en excepciones, lo cual indica posible explotación.
3. Restringir accesos administrativos a redes seguras, aplicar autenticación multifactor y segmentación de red.
4. Implementar reglas de seguridad en WAF y EDR para detectar intentos de deserialización y ejecución de comandos inusuales.

Prioridad: Crítica.

Ampliar Información:

- https://thehackernews.com/2025/09/fortra-releases-critical-patch-for-cvss.html
- https://www.fortra.com/security/advisories/product-security/fi-2025-012
- https://www.securityweek.com/fortra-patches-critical-goanywhere-mft-vulnerability/

MALWARE

MALTERMINAL (LLM EMBEBIDO EN GPT-4)

Investigadores de SentinelOne han descubierto MalTerminal, el primer malware documentado que integra un modelo de lenguaje (LLM) – GPT-4 en su funcionamiento, marcando un punto de inflexión en la evolución de amenazas. Este hallazgo fue presentado en la conferencia LABScon 2025 y representa el ejemplo más antiguo conocido de malware potenciado por IA generativa.

Resumen técnico:

- MalTerminal.exe: binario para Windows que emplea la API de OpenAI (chat completions, hoy deprecada) para interactuar con GPT-4.
- Funcionalidad dinámica: solicita al operador elegir entre generar un payload de ransomware o un reverse shell, generando el código malicioso en tiempo real.
- Incluye scripts en Python con funciones equivalentes y una herramienta defensiva llamada FalconShield, que utiliza GPT-4 para analizar archivos y producir reportes de malware.
- Por su diseño, el malware no contiene un payload estático, lo que dificulta la detección mediante firmas tradicionales, ya que el código se obtiene bajo demanda desde el modelo de IA.

Impacto potencial:

- Generación dinámica de ransomware o shells inversos que evaden controles estáticos.
- Mayor adaptabilidad y personalización de ataques, reduciendo la efectividad de defensas basadas en patrones.
- Potencial uso futuro por actores criminales o APTs para automatizar la creación de variantes maliciosas únicas.
- Phishing potenciado con prompt injection: técnicas que ocultan instrucciones en correos HTML para engañar a sistemas de seguridad basados en IA.

Recomendaciones de mitigación:

1. Monitorear el uso de APIs de IA en entornos corporativos, aplicando restricciones sobre conexiones externas desde binarios desconocidos.
2. Reforzar la protección frente a scripts Python no autorizados y ejecutables sospechosos con EDR avanzado y análisis de comportamiento.
3. Implementar políticas de gobernanza de claves API, con rotación periódica y controles de acceso estrictos.

4. Fortalecer las defensas anti-phishing, considerando la manipulación semántica que introducen los LLM en correos y sitios web.
5. Adoptar principios de Zero Trust, MFA y segmentación de red para limitar movimientos laterales.

Prioridad: Importante.

Ampliar Información:

- https://thehackernews.com/2025/09/researchers-uncover-gpt-4-powered.html
- https://unaaldia.hispasec.com/2025/09/malterminal-el-primer-malware-que-integra-gpt-4-para-crear-ransomware-y-evadir-defensas.html
- https://www.esecurityplanet.com/news/malterminal-malware-gpt-4/

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

UNC1549 (IRÁN) COMPROMETE 34 DISPOSITIVOS EN TELECOMUNICACIONES

Una investigación de PRODAFT reveló una nueva campaña de ciberespionaje atribuida al grupo iraní UNC1549 (alias Subtle Snail, TA455), vinculada al IRGC, que comprometió 34 dispositivos en 11 compañías de telecomunicaciones en Canadá, Francia, EAU, Reino

Unido y EE. UU.. El ataque se apoyó en señuelos de empleo en LinkedIn y en el uso del backdoor MINIBIKE, desplegado mediante técnicas de DLL side-loading y con comunicación C2 a través de infraestructura Azure para evadir detección.

Resumen técnico:

- Vector inicial: suplantación de reclutadores en LinkedIn → contacto con perfiles técnicos → spear-phishing de validación de correos → falsa entrevista en dominio señuelo → descarga de ZIP con ejecutable malicioso.
- Carga útil: ejecutable que activa MINIBIKE (SlugResin) mediante side-loading.
- Capacidades de MINIBIKE: Recolección de info del sistema, Keylogging, captura de portapapeles y screenshots, Robo de credenciales de Microsoft Outlook y navegadores (Chrome, Brave, Edge), Desencriptado de contraseñas en Chrome mediante abuso de la App-Bound Encryption y Persistencia con claves de Registro y técnicas anti-análisis.
- Infraestructura: más de 125 subdominios en Azure (App Services) usados como proxy C2, ocultando el tráfico en servicios cloud legítimos.

Impacto potencial:

- Espionaje estratégico en telecomunicaciones con acceso a metadatos de red, VPNs y credenciales sensibles.
- Persistencia de largo plazo con capacidad de expansión hacia otros sectores críticos (aeroespacial y defensa).
- Uso de infraestructura cloud legítima que dificulta la detección con bloqueos tradicionales.
- Riesgo de movimientos laterales y exfiltración masiva de información confidencial.

Recomendaciones para mitigar el riesgo:

- Seguridad en endpoints: aplicar WDAC/AppLocker, bloquear DLL hijacking y monitorear cargas no firmadas.

- Control de egress: restringir conexiones a servicios cloud a dominios aprobados y revisar tráfico hacia *.azurewebsites.net.
- Controles de identidad: MFA resistente a phishing, Conditional Access y rotación de credenciales ante cualquier incidente.
- Gestión de navegadores y secretos: forzar perfiles corporativos, deshabilitar almacenes locales de contraseñas y vigilar intentos de desencriptado.
- Concienciación: entrenar personal técnico frente a señuelos de “RR. HH.” y verificar ofertas por canales alternativos.
- Hunting e IOCs: buscar persistencia de MINIBIKE/MINIBUS, claves de Registro sospechosas y patrones de tráfico asociados.

Prioridad: Urgente.

Ampliar Información:

- https://thehackernews.com/2025/09/unc1549-hacks-34-devices-in-11-telecom.html
- https://unaaldia.hispasec.com/2025/09/unc1549-ofertas-falsas-linkedin-telecom-34-equipos.html