GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °1725

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	1	2	0
MALWARE	0	0	1
NOTICIAS DE CIBERSEGURIDAD	0	0	2

VULNERABILIDADES

Múltiples vulnerabilidades en productos VMware Tanzu

El 30 de abril de 2025, Broadcom publicó un boletín de seguridad informando sobre ocho vulnerabilidades en productos de VMware Tanzu, incluyendo Tanzu Application Service, Spring Framework y Greenplum. Una de estas vulnerabilidades es de severidad crítica, dos son de severidad alta y las restantes de severidad media. Estas fallas podrían permitir desde la ejecución remota de código hasta ataques de denegación de servicio (DoS) y escaladas de privilegios.

Los CVE relacionados a este compromiso de seguridad son:

- CVE-2025-24813: Vulnerabilidad crítica en Apache Tomcat que permite ejecución remota de código sin autenticación mediante la funcionalidad de PUT parcial
- CVE-2024-22262: Vulnerabilidad de redirección abierta en Spring Framework que podría facilitar ataques de phishing.

- CVE-2025-22866: Afecta a los componentes de red de Tanzu Platform for Cloud Foundry, permitiendo acceso no autorizado o interceptación de datos en segmentos de red aislados.

Recomendaciones de mitigación:

1. Aplicar actualizaciones de seguridad: Actualizar todos los productos afectados a las versiones más recientes proporcionadas por VMware/Broadcom.
2. Revisar configuraciones de seguridad: Asegurarse de que las configuraciones predeterminadas, como la funcionalidad de PUT parcial en Apache Tomcat, estén deshabilitadas si no son necesarias
3. Monitorear actividad sospechosa: Implementar sistemas de detección y respuesta ante intrusiones para identificar posibles intentos de explotación
4. Capacitar al personal: Educar a los usuarios sobre los riesgos asociados a ataques de phishing y la importancia de no interactuar con enlaces sospechosos

Prioridad: Critica.

Ampliar Información:

- https://www.incibe.es/incibe-cert/alerta-temprana/avisos/multiples-vulnerabilidades-en-productos-tanzu-de-vmware
- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25536
- https://rewterz.com/threat-advisory/cve-2024-22262-vmware-tanzu-spring-framework-vulnerability

---

Múltiples vulnerabilidades en Commvault permiten ejecución remota de código y control del servidor

El 29 de abril de 2025, INCIBE-CERT emitió una alerta sobre dos vulnerabilidades graves en productos de Commvault, una de las cuales ha sido activamente explotada y catalogada por la CISA en su listado de vulnerabilidades conocidas explotadas (KEV). Ambas fallas

afectan a versiones específicas de Commvault Command Center y su servidor web, permitiendo a atacantes ejecutar código malicioso y comprometer completamente los sistemas afectados.

Los CVE relacionados a este compromiso de seguridad son:

- CVE-2025-34028 (Crítica, CVSS 10.0): Vulnerabilidad de salto de directorio en Commvault Command Center (versiones 11.38.0 a 11.38.19) que permite a un atacante no autenticado subir archivos ZIP maliciosos. Al descomprimirse, estos archivos pueden ejecutar código arbitrario en el servidor, comprometiendo completamente el entorno.
- CVE-2025-3928 (Alta): Vulnerabilidad en el servidor web de Commvault que permite a un atacante autenticado comprometer el servidor mediante la creación y ejecución de webshells. Esta falla ha sido activamente explotada y añadida al catálogo KEV de la CISA.

Recomendaciones de mitigación:

- Actualizar a versiones corregidas:
  - Para CVE-2025-34028: Actualizar a las versiones 11.38.20 o 11.38.25.
  - Para CVE-2025-3928: Actualizar a las versiones 11.36.46, 11.32.89, 11.28.141 o 11.20.217, según corresponda.
- Restringir el acceso externo: Si la actualización inmediata no es posible, se recomienda aislar el Command Center de accesos externos para mitigar riesgos.
- Monitorear actividad sospechosa: Implementar sistemas de detección de intrusiones para identificar posibles actividades maliciosas relacionadas con estas vulnerabilidades.
- Revisar configuraciones de seguridad: Asegurarse de que las configuraciones predeterminadas no expongan innecesariamente servicios críticos a redes externas.

Prioridad: Urgente.

Ampliar Información:

- https://www.incibe.es/incibe-cert/alerta-temprana/avisos/multiples-vulnerabilidades-en-commvault
- https://www.cisa.gov/news-events/alerts/2025/04/28/cisa-adds-three-known-exploited-vulnerabilities-catalog
- https://documentation.commvault.com/securityadvisories/

Alerta en impresoras Epson: vulnerabilidad de escalada de privilegios locales (CVE-2025-42598)

El 28 de abril de 2025, se identificó una vulnerabilidad de alta severidad en los controladores de impresoras Epson para sistemas Windows configurados en idiomas distintos al inglés. Esta falla, catalogada como CVE-2025-42598, permite a un atacante local ejecutar código arbitrario con privilegios de SYSTEM, el nivel más alto en Windows. El investigador Erkan Ekici descubrió esta vulnerabilidad, que afecta a múltiples modelos de impresoras Epson

Los CVE relacionados a este compromiso de seguridad son:

CVE-2025-42598: Vulnerabilidad en los controladores de impresoras Epson para Windows que permite la ejecución de código con privilegios elevados mediante la sobrescritura de archivos DLL en sistemas configurados en idiomas distintos al inglés

Recomendaciones de mitigación:

1. Actualizar los controladores de impresora: Utilizar la herramienta Epson Software Updater para instalar las actualizaciones de seguridad proporcionadas por el fabricante.
2. Revisar las configuraciones de idioma: Asegurarse de que los sistemas Windows estén configurados correctamente y considerar las implicaciones de seguridad al cambiar el idioma del sistema.

3. Monitorear la actividad del sistema: Implementar soluciones de monitoreo para detectar comportamientos anómalos que puedan indicar intentos de explotación de esta vulnerabilidad.

Prioridad: Urgente.

Ampliar Información:

- https://www.epson.eu/en_EU/faq/KA-01896/contents?loc=en-us
- https://www.incibe.es/incibe-cert/alerta-temprana/avisos/escalada-de-privilegios-locales-en-impresoras-de-epson

---

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

Alerta de Seguridad: DoubleClickjacking – Nuevo ataque que explota doble clics para secuestrar cuentas

Investigadores de ciberseguridad han identificado una nueva técnica de ataque denominada DoubleClickjacking, que representa una evolución del tradicional clickjacking. Este método malicioso aprovecha la secuencia de doble clic realizada por los usuarios para ejecutar acciones no autorizadas, como la toma de control de cuentas o la realización de transacciones sin el consentimiento del usuario.

A diferencia del clickjacking convencional, que generalmente requiere un solo clic, el DoubleClickjacking inserta un elemento malicioso entre el primer y segundo clic del usuario. Esto permite a los atacantes manipular la interfaz de usuario y engañar al usuario para que realice acciones no deseadas.

Recomendaciones para mitigar el riesgo:

- Implementar encabezados de seguridad: Utilizar políticas como X-Frame-Options y Content-Security-Policy para prevenir la carga de contenido en iframes no autorizados.infosecurity-magazine.com
- Validación de acciones sensibles: Requerir confirmaciones adicionales para acciones críticas, como transferencias de fondos o cambios de contraseña.
- Monitoreo de comportamiento del usuario: Detectar patrones inusuales de clics que puedan indicar intentos de DoubleClickjacking.
- Educación y concienciación: Informar a los usuarios sobre los riesgos de hacer clic en elementos desconocidos o sospechosos, incluso en sitios web legítimos.
- Actualización de navegadores y sistemas: Mantener todos los sistemas y navegadores actualizados para beneficiarse de las últimas protecciones de seguridad.

Prioridad: Importante.

Ampliar Información:

- https://www.portafolio.co/tecnologia/doubleclickjacking-el-nuevo-ciberataque-del-que-puede-ser-victima-como-evitarlo-628682
- https://www.bitdefender.com/en-us/blog/hotforsecurity/emerging-doubleclickjacking-threat-exploits-double-clicks-for-account-hijacking
- https://thehackernews.com/2025/01/new-doubleclickjacking-exploit-bypasses.html

---

Recomendaciones generales sobre malware:

Para protegerse contra malware, es esencial:

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

Alerta de Soporte: Microsoft ofrecerá actualizaciones de seguridad pagas para Windows 10 hasta 2028

Microsoft ha anunciado que, tras el fin del soporte oficial de Windows 10 el 14 de octubre de 2025, los usuarios podrán optar por un programa de Actualizaciones de Seguridad Extendidas (ESU) para continuar recibiendo parches críticos y de seguridad importantes. Este programa estará disponible por un período de hasta tres años, es decir, hasta octubre de 2028.

Por primera vez, los usuarios domésticos podrán acceder a este servicio, con un costo de $30 USD por el primer año. Las empresas, por su parte, pagarán $61 USD el primer año, con incrementos en los años subsiguientes. Es importante destacar que este programa no incluye nuevas funciones, correcciones de errores no relacionados con seguridad ni soporte técnico

Prioridad: Importante.

Ampliar Información:

- https://www.theverge.com/2024/10/31/24284398/microsoft-windows-10-extended-security-updates-consumer-pricing
- https://www.microsoft.com/es-es/windows/end-of-support?r=1
- https://www.genbeta.com/windows/hay-solucion-para-seguir-usando-windows-10-durante-7-anos-microsoft-quien-ofrece

---

Alerta: RansomHub desaparece repentinamente; afiliados migran a Qilin y DragonForce

El 1 de abril de 2025, la infraestructura en línea de RansomHub, una prominente operación de ransomware como servicio (RaaS), se desconectó inesperadamente, generando incertidumbre entre sus afiliados y provocando una migración hacia otros grupos como Qilin y DragonForce.

Resumen de la situación:

- Origen y ascenso: RansomHub emergió en febrero de 2024, sucediendo a grupos como LockBit y BlackCat. Se destacó por su modelo atractivo para afiliados, ofreciendo divisiones de pagos lucrativas y soporte para múltiples plataformas, incluyendo Windows, Linux, FreeBSD y ESXi, además de arquitecturas x86, x64 y ARM.

- Desaparición y consecuencias: La desconexión abrupta de su infraestructura dejó a los afiliados sin acceso a herramientas esenciales, como el panel de configuración del ransomware y el sitio de filtración de datos. Esto llevó a una migración hacia otros grupos RaaS, notablemente Qilin, que duplicó sus publicaciones en su sitio de filtración desde febrero, y DragonForce, que afirmó haber absorbido a RansomHub en su "Cartel de Ransomware DragonForce".
- Conflictos internos: Informes indican que algunos afiliados perdieron acceso a los portales de comunicación de RansomHub antes de su desaparición, sugiriendo posibles conflictos internos.

Recomendaciones para organizaciones:

1. Estar atentos a posibles ataques de grupos emergentes como Qilin y DragonForce, que podrían utilizar herramientas y tácticas heredadas de RansomHub.
2. Revisar y fortalecer las medidas de seguridad existentes, asegurando la detección y prevención de técnicas asociadas con RaaS.
3. Educar al personal sobre las amenazas actuales y las mejores prácticas para evitar infecciones por ransomware.

Prioridad: Importante.

Ampliar Información:

- https://www.scworld.com/news/ransomhub-affiliates-scramble-amid-apparent-internal-conflict
- https://thehackernews.com/2025/04/ransomhub-went-dark-april-1-affiliates.html