GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º1425

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

VULNERABILIDADES

Vulnerabilidades en Cisco Enterprise Chat e Email y Cisco AnyConnect VPN

Cisco ha reportado vulnerabilidades críticas en sus productos que podrían ser explotadas para causar ataques de denegación de servicio (DoS). En los dispositivos Meraki MX y Z Series con Cisco AnyConnect VPN, un atacante remoto autenticado puede interrumpir las sesiones SSL VPN activas, forzando a los usuarios a Re autenticarse. Adicionalmente, el módulo de mensajería de Cisco Enterprise Chat and Email (ECE) permite que un atacante no autenticado envíe solicitudes maliciosas que paralicen la aplicación. Ambas fallas comprometen seriamente la disponibilidad del servicio, afectando la continuidad operativa y la experiencia del usuario. Cisco recomienda aplicar las actualizaciones de seguridad correspondientes para mitigar estos riesgos.

Los CVE relacionados a este compromiso de seguridad son:

- CVE-2025-20139
- CVE-2025-20212

Ambas vulnerabilidades presentan un riesgo significativo para la disponibilidad de servicios críticos en organizaciones que utilizan plataformas Cisco para atención al cliente y acceso remoto. Aunque no se han detectado exploits públicos activos al momento del reporte, la facilidad de explotación y el impacto directo justifican una categorización de prioridad alta. Se recomienda actuar con inmediatez para mitigar posibles ataques que comprometan la continuidad operativa.

Prioridad: Urgente.

Ampliar Información:

https://ciberseguridad.euskadi.eus/noticia/2025/aviso-de-seguridad-vulnerabilidades-en-cisco-enterprise-chat-e-email-y-cisco-anyconnect-vpn/webcyb00-contcibglos/es/

Vulnerabilidad explotada en Apache Tomcat

Durante la primera semana de abril, se ha detectado una vulnerabilidad identificada como CVE-2025-24813 en Apache Tomcat de alto riesgo en un componente ampliamente utilizado por muchas organizaciones

Esta falla, clasificada como crítica, podría ser utilizada por ciberdelincuentes para:

- Insertar archivos maliciosos en los servidores
- Acceder a información confidencial
- Tomar control remoto del sistema afectado

En términos prácticos, si esta vulnerabilidad es aprovechada por un atacante, podría dejar expuestos documentos privados o datos sensibles, permitir que software malicioso se ejecute sin autorización, interrumpir operaciones internas o servicios digitales de la empresa

Las versiones de Apache Tomcat afectadas son las siguientes versiones:

- 11.0.0-M1 hasta 11.0.2

- 10.1.0-M1 hasta 10.1.34
- 9.0.0-M1 hasta 9.0.98

Este tipo de ataque no requiere acceso físico, puede hacerse a través de internet además permite comprometer la seguridad del sistema de forma silenciosa y podría causar interrupciones, fugas de información o manipulación de datos.

Como recomendación para mitigar el riesgo: Los equipos técnicos deben aplicar de inmediato las actualizaciones oficiales que corrigen esta falla. Las versiones actualizadas (11.0.3, 10.1.35 o 9.0.99) ya están disponibles y son esenciales para proteger los entornos digitales de la organización.

Prioridad: Urgente.

Ampliar Información:

https://ciberseguridad.euskadi.eus/noticia/2025/aviso-de-seguridad-vulnerabilidad-explotada-en-apache-tomcat/webcyb00-contcibglos/es/

Recomendaciones generales sobre vulnerabilidades:

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

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

NOTICIAS DE CIBERSEGURIDAD

El sitio de filtración de la dark web del ransomware Everest fue desfigurado y ahora está fuera de línea

Durante el fin de semana, el sitio de filtración en la dark web utilizado por la banda de ransomware Everest fue intervenido y desactivado por un atacante desconocido. El sitio fue reemplazado temporalmente con un mensaje sarcástico que decía:

"No cometas delitos, EL CRIMEN ES MALO xoxo desde Praga"

Actualmente, el sitio se encuentra fuera de línea y muestra un error que indica que la dirección Onion (de la red Tor) ya no está disponible.

Posible vector de ataque, aunque la autoría del ataque sigue sin confirmarse, expertos en ciberseguridad como Tammy Harper (Flare) sugieren que la banda Everest podría haber usado una plantilla de WordPress vulnerable, lo que habría facilitado la desfiguración y caída del sitio.

Contexto del grupo Everest, desde su aparición en 2020 Everest ha evolucionado de simples extorsiones por robo de datos a ejecutar ataques de doble extorsión:

- Roban información confidencial.
- Cifran los sistemas de la víctima usando ransomware.
- Amenazan con publicar los datos si no reciben un rescate.

Everest también opera como intermediario de acceso inicial, vendiendo el acceso a redes comprometidas a otros grupos criminales lo que aumenta el riesgo de ataques posteriores.

Prioridad: Importante.

Ampliar Información:

https://www.bleepingcomputer.com/news/security/everest-ransomwares-dark-web-leak-site-defaced-now-offline/

Windows 11 24H2 bloqueado en PC con pantallas azules de la muerte (BSOD) del controlador de ofuscación de código

Microsoft ha identificado una incompatibilidad crítica entre la actualización de Windows 11 versión 24H2 y el controlador 'sprotect.sys', desarrollado por SenseShield Technology Co. Este controlador se utiliza en diversas soluciones de seguridad y software empresarial para proporcionar funciones de cifrado y protección de datos. La presencia de este controlador en sistemas que intentan actualizar a Windows 11 24H2 ha provocado errores graves, conocidos como "pantallas azules o negras de la muerte" (BSOD), resultando en fallos completos del sistema.

Actualmente Microsoft ha optado por implementar un bloqueo de compatibilidad para impedir que los sistemas con el controlador 'sprotect.sys' actualicen a la versión 24H2 de Windows 11. Este bloqueo busca prevenir interrupciones operativas y mantener la estabilidad del sistema.

Se han brindado ciertas recomendaciones para las Organizaciones las cuales son.

- Identificación del Controlador Afectado: Verificar si los sistemas utilizan el controlador 'sprotect.sys'. Esto puede hacerse revisando la lista de controladores instalados o consultando con los proveedores de software de seguridad implementados en la organización.

- Postergación de la Actualización: Evitar la actualización a Windows 11 24H2 en sistemas que tengan el controlador mencionado hasta que se disponga de una solución oficial. Forzar la actualización podría resultar en fallos críticos del sistema.

- Mantenerse Informado: Seguir las comunicaciones oficiales de Microsoft y SenseShield Technology para obtener actualizaciones sobre la resolución del problema y las recomendaciones adicionales.

Prioridad: Importante.

Ampliar Información:

https://www.bleepingcomputer.com/news/security/windows-11-24h2-blocked-on-pcs-with-code-obfuscation-driver-bsods/