GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º5025

TLP:GREEN
TRAFFIC LIGHT PROTOCOL
https://www.first.org/tlp/

BOLETÍN CIBERSEGURIDAD
SEMANAL EDICIÓN º5025

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	0	1	0

VULNERABILIDADES

FORTINET — BYPASS DE AUTENTICACIÓN SSO CRÍTICO Y MÚLTIPLES VULNERABILIDADES (CVE-2025-59718/19)

Fortinet ha emitido una alerta de máxima prioridad tras descubrir vulnerabilidades críticas que afectan a la gestión de identidad en sus dispositivos. Los fallos, rastreados como CVE-2025-59718 y CVE-2025-59719, permiten a atacantes remotos eludir la autenticación del inicio de sesión único (SSO) de FortiCloud debido a una verificación criptográfica incorrecta. Además, se han solucionado vulnerabilidades de ejecución remota de código y path traversal en otros componentes del ecosistema.

Resumen técnico:

- Identificadores: CVE-2025-59718 (FortiOS, FortiProxy, FortiSwitchManager) y CVE-2025-59719 (FortiWeb).
- Vector de ataque: Un atacante no autenticado envía un mensaje de respuesta SAML manipulado al dispositivo objetivo.
- Causa raíz: Verificación incorrecta de la firma criptográfica (CWE-347) durante el proceso de "handshake" de autenticación SSO.
- Condición de explotación: La función "Allow administrative login using FortiCloud SSO" debe estar habilitada (esta opción suele activarse por defecto al registrar el equipo en FortiCare).
- Versiones afectadas:
- FortiOS: Ramas 7.6 (7.6.0-7.6.3), 7.4 (7.4.0-7.4.8), 7.2 (7.2.0-7.2.11) y 7.0 (7.0.0-7.0.17).
- FortiProxy: Versiones anteriores a 7.6.4, 7.4.11, 7.2.15 y 7.0.22.
- FortiWeb: Versiones 8.0.0, 7.6.x hasta 7.6.4, y 7.4.x hasta 7.4.9.

Impacto potencial:

- Elusión de autenticación: Acceso administrativo completo a la interfaz de gestión del dispositivo sin necesidad de credenciales válidas.
- Ejecución remota de código (RCE): En combinación con otras fallas parchadas (como CVE-2025-53949 en FortiSandbox), un atacante podría ejecutar comandos arbitrarios en el sistema operativo subyacente.
- Compromiso de la red: Al tomar control del firewall o proxy perimetral, el atacante puede interceptar tráfico, modificar políticas de seguridad y facilitar movimientos laterales hacia la red interna.
- Exfiltración de configuración: Acceso a archivos de configuración sensibles, incluyendo hashes de contraseñas y llaves VPN.

Recomendaciones de mitigación:

1. Actualización Inmediata: Instalar las versiones parcheadas proporcionadas por el fabricante:
   FortiOS: Actualizar a 7.6.4, 7.4.9, 7.2.12 o 7.0.18.
   FortiProxy: Actualizar a 7.6.4, 7.4.11, 7.2.15 o 7.0.22.

FortiWeb: Actualizar a 8.0.1, 7.6.5 o 7.4.10.

2. Solución temporal (Workaround): Si no es posible actualizar inmediatamente, deshabilitar la función de inicio de sesión administrativo vía FortiCloud SSO mediante la CLI:
   config system global
   set admin-forticloud-sso-login disable
   end
3. Revisión de Logs: Auditar los registros de acceso en busca de inicios de sesión administrativos inusuales provenientes de direcciones IP desconocidas o intentos fallidos de SAML.

Prioridad: Crítica.

Ampliar información:

- https://www.fortiguard.com/psirt
- https://thehackernews.com/2025/12/fortinet-ivanti-and-sap-issue-urgent.html
- https://arcticwolf.com/resources/blog/cve-2025-59718-and-cve-2025-59719/
- https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/critical-vulnerabilities-in-multiple-fortinet-products-forticloud-sso-login-authentication-bypass
- https://ciberseguridad.euskadi.eus/noticia/2025/vulnerabilidades-criticas-en-fortios-fortiweb-y-otros-productos/webcyb00-contcibglos/es/

IVANTI — FALLA CRÍTICA EN ENDPOINT MANAGER (EPM) PERMITE EJECUCIÓN REMOTA DE CÓDIGO VÍA XSS (CVE-2025-10573)

Ivanti ha lanzado una actualización de seguridad urgente para su solución Endpoint Manager (EPM) con el fin de corregir cuatro vulnerabilidades, destacando un fallo crítico que permite a atacantes no autenticados tomar el control de sesiones administrativas. La vulnerabilidad principal, catalogada como un Cross-Site Scripting (XSS) almacenado, facilita la ejecución de código JavaScript arbitrario en el contexto de la sesión del administrador, lo que puede derivar en un compromiso total del servidor de gestión.

Además, se han parchado vulnerabilidades de escritura de archivos arbitrarios y elusión de verificaciones criptográficas.

Resumen técnico:

- Identificador principal: CVE-2025-10573 (CVSS 9.6 - Crítica).
- Vulnerabilidades adicionales corregidas:
- CVE-2025-13659 (CVSS 8.8): Escritura de archivos arbitrarios debido a verificaciones insuficientes en recursos de código gestionados dinámicamente.
- CVE-2025-13662 (CVSS 7.8): Ejecución remota de código por verificación incorrecta de firmas criptográficas.
- CVE-2025-13661 (CVSS 7.1): Vulnerabilidad de Path Traversal que permite almacenar archivos fuera de los directorios permitidos.
- Vector de ataque (CVE-2025-10573): Un atacante remoto no autenticado envía datos de escaneo de dispositivos falsos a la API incomingdata del servidor EPM.
- Mecanismo: El servidor procesa estos datos (archivos de escaneo tipo clave=valor) sin la debida sanitización a través del binario CGI postcgi.exe, inyectando payloads de JavaScript malicioso en la base de datos.
- Detonante: La ejecución del código ocurre cuando un administrador visualiza pasivamente el panel de control (dashboard) "envenenado" durante sus tareas rutinarias.
- Versiones afectadas: Ivanti Endpoint Manager (EPM) versiones anteriores a 2024 SU4 SR1.

Impacto potencial:

- Secuestro de sesión (Session Hijacking): El atacante obtiene el control total de la sesión del administrador, permitiéndole gestionar endpoints, desplegar software y modificar configuraciones.
- Ejecución Remota de Código (RCE): Mediante el acceso administrativo o explotando las vulnerabilidades adicionales (CVE-2025-13662), el atacante puede ejecutar comandos en el servidor central (Core Server).

- Compromiso de la cadena de suministro interna: Al controlar el EPM, el atacante podría utilizar la infraestructura de gestión para distribuir malware a todos los dispositivos gestionados por la organización.

Recomendaciones de mitigación:

1. Actualización Inmediata: Instalar la versión Ivanti EPM 2024 SU4 SR1 o superior, que soluciona tanto el XSS crítico como los fallos de escritura de archivos.
2. Restricción de Acceso a Red: Asegurar que el servidor Core de EPM no sea accesible directamente desde Internet pública, limitando el acceso solo a redes de gestión confiables o mediante VPN.
3. Segmentación: Implementar una segmentación estricta para aislar el servidor de gestión de endpoints del resto de la red corporativa crítica.

Prioridad: Crítica.

Ampliar información:

- https://www.csa.gov.sg/alerts-and-advisories/alerts/al-2025-114/
- https://www.rapid7.com/blog/post/cve-2025-10573-ivanti-epm-unauthenticated-stored-cross-site-scripting-fixed/
- https://securityaffairs.com/185508/hacking/ivanti-warns-customers-of-new-epm-flaw-enabling-remote-code-execution.html
- https://thehackernews.com/2025/12/fortinet-ivanti-and-sap-issue-urgent.html
  - https://www.heise.de/en/news/Ivanti-Patches-Critical-Security-Vulnerability-in-Endpoint-Manager-11110509.html

SAP — ACTUALIZACIÓN CRÍTICA DE DICIEMBRE: INYECCIÓN DE CÓDIGO Y FALLOS EN COMMERCE CLOUD (CVE-2025-42880)

SAP ha publicado su paquete de seguridad de diciembre abordando 14 vulnerabilidades, destacando tres de severidad crítica que afectan a componentes centrales de la infraestructura empresarial. La falla más grave, con una puntuación casi máxima (CVSS

9.9), reside en SAP Solution Manager, permitiendo a atacantes autenticados inyectar código malicioso y tomar el control total del sistema. Adicionalmente, se han corregido vulnerabilidades críticas en SAP Commerce Cloud y el controlador SAPj Connect.

Resumen técnico:

- Identificadores principales:
- CVE-2025-42880 (CVSS 9.9): Inyección de código en SAP Solution Manager ST 720.
- CVE-2025-55754 (CVSS 9.6): Múltiples vulnerabilidades en Apache Tomcat que afectan a SAP Commerce Cloud.
- CVE-2025-42928 (CVSS 9.1): Deserialización insegura en SAP jConnect.
- Vector de ataque (Solution Manager): Un atacante autenticado aprovecha la falta de saneamiento de entradas al invocar un módulo de función habilitado remotamente para insertar código malicioso.
- Vector de ataque (Commerce Cloud): Inyección de secuencias de escape ANSI en los registros (logs), lo que permite manipular la consola y el portapapeles para engañar a administradores.
- Vector de ataque (jConnect): Un usuario con privilegios elevados envía entradas especialmente diseñadas (crafted inputs) para lograr la ejecución de código.
- Versiones afectadas:
- SAP Solution Manager: ST 720.
- SAP Commerce Cloud: HY_COM 2205, COM_CLOUD 2211, COM_CLOUD 2211-JDK21.
- SAP jConnect: SDK para ASE versiones 16.0.4 y 16.1.

Impacto potencial:

- Control total del sistema (Solution Manager): Dada la centralidad de este componente en la gestión del ciclo de vida SAP, su compromiso otorga al atacante control total sobre la confidencialidad, integridad y disponibilidad del entorno.
- Ejecución Remota de Código (RCE): Posible en los tres vectores críticos, permitiendo a los atacantes ejecutar comandos arbitrarios en los servidores afectados.
- Movimiento lateral: El compromiso de Solution Manager facilita el acceso a otros sistemas satélites conectados en la red empresarial.

Recomendaciones de mitigación:

1. Parcheo Prioritario: Aplicar inmediatamente las notas de seguridad de diciembre desde el portal de soporte de SAP, priorizando Solution Manager y Commerce Cloud.
2. Gestión de Dependencias: Para Commerce Cloud, asegurar que los componentes subyacentes de Apache Tomcat estén actualizados a versiones seguras (11.0.11, 10.1.45 o 9.0.109).
3. Restricción de Privilegios: Revisar y limitar los privilegios de usuarios con acceso a módulos de función remota y bases de datos conectadas vía JDBC.

Prioridad: Crítica.

Ampliar información:

- https://www.csa.gov.sg/alerts-and-advisories/alerts/al-2025-113/
- https://thehackernews.com/2025/12/fortinet-ivanti-and-sap-issue-urgent.html
- https://bitlifemedia.com/2025/12/sap-corrige-tres-fallos-criticos-con-riesgo-de-ejecucion-remota-dentro-de-un-total-de-14-vulnerabilidades/
- https://ciberseguridad.euskadi.eus/noticia/2025/actualizacion-de-seguridad-de-sap-diciembre-2025/webcyb00-contcibglos/es/
- https://www.bleepingcomputer.com/news/security/sap-fixes-three-critical-vulnerabilities-across-multiple-products/

MALWARE

SILVER FOX — DISTRIBUCIÓN MASIVA DE VALLEYRAT MEDIANTE SITIOS DE DESCARGA FALSOS

Investigadores de seguridad han identificado una sofisticada campaña del grupo APT chino Silver Fox (también conocido como Void Arachne), activa desde noviembre de 2025. El grupo emplea técnicas de envenenamiento de motores de búsqueda (SEO Poisoning) para distribuir instaladores troyanizados de software popular como Microsoft Teams, Google Chrome y Telegram, desplegando el malware ValleyRAT. Una característica distintiva es el uso de tácticas de "falsa bandera", imitando a actores de amenazas rusos para dificultar la atribución.

Resumen técnico:

- Actor de Amenaza: Silver Fox (APT alineado con China).
- Vector de Infección: Sitios web falsos posicionados mediante SEO (ej. teamscn[.]com) que suplantan portales de descarga legítimos.
- Archivos Troyanizados: Archivos ZIP (ej. MSTчamsSetup.zip) que contienen instaladores legítimos empaquetados junto con componentes maliciosos.
- Técnica de Falsa Bandera: Uso deliberado de caracteres cirílicos en nombres de archivos y recursos en idioma ruso dentro de los binarios (Verifier.exe) para simular origen ruso.
- Mecanismo de Evasión (Defense Evasion):
- El instalador ejecuta un comando de PowerShell para excluir unidades completas del escaneo de Windows Defender: powershell.exe -ExecutionPolicy Bypass -Command Add-MpPreference -ExclusionPath C:\, D:\, E:\, F:\.
- Escaneo de procesos para detectar antivirus chinos como "360 Total Security".
- Ejecución: Utiliza la técnica de DLL Sideloading (carga lateral) mediante procesos legítimos como rundll32.exe para cargar la carga útil de ValleyRAT en memoria.

Impacto potencial:

- Compromiso Total del Endpoint: ValleyRAT otorga control remoto completo sobre el sistema infectado.
- Espionaje y Exfiltración: Capacidad para realizar capturas de pantalla, keylogging (registro de teclas), acceso a micrófono/cámara y robo de archivos sensibles.
- Persistencia a largo plazo: El malware establece tareas programadas y modificaciones de registro para sobrevivir a reinicios.
- Riesgo Financiero y Operativo: Silver Fox realiza tanto espionaje estatal como fraude financiero, aumentando el riesgo de robo de credenciales bancarias y datos corporativos.

Recomendaciones de mitigación:

1. Restricción de Software: Implementar políticas que impidan a los usuarios descargar e instalar software desde internet; utilizar repositorios corporativos centralizados.
2. Monitoreo de PowerShell: Habilitar y auditar el registro de bloques de scripts de PowerShell (Event ID 4104) buscando comandos Add-MpPreference sospechosos.
3. Verificación de Fuentes: Educar a los usuarios sobre los riesgos de descargar software desde enlaces patrocinados en buscadores; verificar siempre la firma digital de los instaladores.
4. Bloqueo de IoCs: Bloquear dominios conocidos como teamscn[.]com y ntpckj[.]com en el firewall perimetral.

Prioridad: Urgente.

Ampliar información:

- https://www.cybersecurity-help.cz/blog/5108.html
- https://thehackernews.com/2025/12/silver-fox-uses-fake-microsoft-teams.html
- https://reliaquest.com/blog/threat-spotlight-silver-foxs-russian-ruse-fake-microsoft-teams-attack/
- https://www.siteguarding.com/security-blog/seo-poisoning-attack-threat-actors-deploy-fake-microsoft-teams-installer-to-distribute-valleyrat-malware/
- https://cyberpress.org/fake-microsoft-teams-installers/
- https://darknetsearch.com/knowledge/news/en/silver-fox-malware-7-key-insights-revealed-in-this-urgent-cyberattack-report/

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

REACT2SHELL — HACKERS CHINOS INICIAN EXPLOTACIÓN MASIVA DE VULNERABILIDAD CRÍTICA EN REACT Y NEXT.JS

Apenas horas después de su divulgación pública, dos grupos de ciber espionaje vinculados a China, conocidos como Earth Lamia y Jackpot Panda, han comenzado a explotar activamente la vulnerabilidad crítica "React2Shell" (CVE-2025-55182). Este fallo, con una puntuación de severidad máxima (CVSS 10.0), permite la ejecución remota de código sin autenticación en servidores que utilizan React Server Components (RSC) y Next.js, tecnologías omnipresentes en el desarrollo web moderno.

Resumen técnico:

- Vulnerabilidad: CVE-2025-55182, apodada "React2Shell".
- Severidad: Crítica (CVSS 10.0) - Ejecución Remota de Código (RCE) no autenticada.
- Mecanismo: Fallo de deserialización insegura en el protocolo "Flight" utilizado por los componentes de servidor de React. Los atacantes envían payloads HTTP manipulados que el servidor procesa erróneamente, ejecutando comandos arbitrarios.
- Actividad en la red: Amazon Web Services (AWS) ha detectado intentos de explotación desde infraestructura asociada a actores estatales chinos, ejecutando comandos de reconocimiento (whoami, id) e intentando leer archivos sensibles (/etc/passwd).
- Alcance: Afecta a versiones de React (19.0.x) y Next.js (14.x, 15.x, 16.x) con configuraciones por defecto. Se estima que millones de aplicaciones podrían estar expuestas.

Impacto potencial:

- Compromiso total del servidor: Los atacantes pueden tomar el control administrativo del servidor web, permitiendo el robo de datos, la instalación de persistencia o el uso del servidor para ataques laterales.
- Automatización del ataque: Ya existen extensiones de navegador y scripts públicos en GitHub que automatizan la explotación, reduciendo la barrera de entrada para ciberdelincuentes menos sofisticados.
- Interrupción de servicios: Grandes proveedores de infraestructura como Cloudflare han reportado breves interrupciones de servicio al implementar reglas de mitigación de emergencia en sus WAF.

Recomendaciones para mitigar el riesgo:

1. Parcheo Urgente: Actualizar inmediatamente a las versiones seguras:
   React: 19.0.1, 19.1.2, o 19.2.1.
   Next.js: Actualizar a las últimas versiones parcheadas de las ramas 15.x y 16.x.
2. Protección WAF: Implementar reglas en el Firewall de Aplicaciones Web para bloquear solicitudes malformadas dirigidas a endpoints de RSC.
3. Monitoreo: Vigilar los logs en busca de solicitudes HTTP inusuales o comandos de sistema ejecutados por el proceso del servidor web.

Prioridad: Urgente.

Ampliar Información:

- https://www.montevideo.com.uy/Ciencia-y-Tecnologia/Hackers-chinos-aprovechan-falla-critica-que-permite-tomar-control-de-paginas-en-segundos-uc945689
- https://www.welivesecurity.com/es/seguridad-digital/react2shell-falla-critica-react-nextjs/
- https://socprime.com/es/blog/react2shell-vulnerability-exploitation/
- https://ciberprisma.org/2025/12/06/cisa-agrega-la-vulnerabilidad-critica-react2shell-a-su-catalogo-kev-tras-confirmarse-explotacion-activa/
- https://thehackernews.com/2025/12/chinese-hackers-have-started-exploiting.html