GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °2426

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

CVE-2026-35273 – ORACLE PEOPLESOFT (EJECUCIÓN REMOTA DE CÓDIGO NO AUTENTICADA - ZERO-DAY)

Se ha divulgado una vulnerabilidad crítica de ejecución remota de código (RCE) que afecta al componente de gestión de entornos de la plataforma Oracle PeopleSoft. El fallo, que fue explotado activamente como un día cero (Zero-Day) antes de la liberación de su parche, permite a atacantes remotos no autenticados tomar el control total de los servidores afectados. Esta vulnerabilidad representa un riesgo extremo debido a que este tipo de plataformas suelen centralizar datos altamente sensibles como registros financieros, recursos humanos y flujos operativos empresariales.

Resumen técnico:

- Identificador principal: CVE-2026-35273.
- Severidad: Crítica (Puntaje base de 9.8 en CVSS v3.1).
- Causa raíz: Un defecto de diseño e inyección lógica en el componente Updates Environment Management, asociado de forma directa con el Environment Management Hub (PSEMHUB), que actúa como un fallo de falsificación de solicitud del lado del servidor (SSRF) y posterior ejecución de código.
- Mecanismo de falla: Un atacante remoto sin credenciales legítimas envía solicitudes HTTP (GET/POST) malformadas y dirigidas explícitamente hacia los endpoints de PSEMHUB. Al procesarse, el sistema ejecuta de forma transparente una cadena de componentes ("gadget chain") que evade los controles de seguridad perimetrales y otorga capacidades de ejecución de comandos a nivel de sistema operativo.
- Estado de explotación: Explotación activa confirmada en el entorno real por parte del grupo de extorsión ShinyHunters (UNC6240) entre finales de mayo y mediados de junio de 2026, afectando masivamente a infraestructuras críticas del sector educativo y corporativo global.
- Versiones afectadas: Oracle PeopleSoft Enterprise PeopleTools en sus versiones 8.61 y 8.62. Las ramas anteriores que ya no cuentan con soporte oficial (End of Support) se evalúan como nativamente vulnerables.

Impacto potencial:

- Ejecución remota de código (RCE) sin autenticación: Permite a actores de amenazas externos e internos tomar control operativo inmediato sobre la suite PeopleSoft de manera invisible, ejecutando instrucciones del sistema con los privilegios del proceso de la aplicación.
- Exfiltración masiva de datos corporativos e institucionales: Al comprometer la base de datos de la plataforma, los atacantes adquieren acceso a información confidencial que incluye datos personales, nóminas, números de identificación/pasaportes, registros financieros e información de propiedad intelectual.
- Movimiento lateral e implantación de infraestructura C2: Los vectores observados demuestran que, tras el acceso inicial, los atacantes despliegan agentes de administración remota (como MeshCentral camuflados como binarios legítimos de Azure) y scripts automatizados de inyección de credenciales por SSH para comprometer otros nodos de la red interna.
- Extorsión cibernética y filtración en la Dark Web: La vinculación de esta campaña con grupos de extorsión financiera implica un riesgo inminente de demandas de rescate (Ransom) bajo la amenaza de publicar la totalidad de los datos robados en sitios de filtraciones públicos (Data Leak Sites), dañando la reputación institucional y activando sanciones legales por brechas de privacidad.

Recomendaciones de mitigación:

1. Aplicación inmediata del parche de seguridad oficial del fabricante: Se urge a los equipos de administración de infraestructura a ingresar a My Oracle Support, descargar de forma prioritaria el "Patch Availability Document" correspondiente y aplicar las actualizaciones de seguridad para PeopleTools 8.61 y 8.62.
2. Desactivación o eliminación del componente de administración expuesto: Siguiendo las directrices del fabricante, se debe deshabilitar por completo el servicio de Environment Management Hub (EMHub) en configuraciones multi-servidor o eliminar de forma definitiva la aplicación PSEMHUB en implementaciones de un solo servidor.
3. Restricción estricta de la exposición en el perímetro de red: Configurar de manera mandatoria reglas en el firewall perimetral y proxies inversos para bloquear cualquier acceso externo proveniente de Internet hacia las rutas sensibles /PSEMHUB/* (especialmente /PSEMHUB/hub) y /PSIGW/HttpListeningConnector.
4. Caza activa de amenazas y auditoría forense de registros: Implementar revisiones exhaustivas en las soluciones SIEM sobre los logs de acceso de WebLogic para identificar peticiones POST anómalas desde IPs externas, escanear el sistema de archivos en busca de archivos .jsp sospechosos creados recientemente en la ruta de PSEMHUB.war y monitorizar tráfico SMB saliente no autorizado por el puerto 445.

Prioridad: Crítica.

Ampliar información:

- https://www.oracle.com/security-alerts/alert-cve-2026-35273.html
- https://thehackernews.com/2026/06/shinyhunters-exploits-oracle-peoplesoft.html
- https://socprime.com/active-threats/cve-2026-35273-oracle-peoplesoft-zero-day-exploited-in-the-wild/
- https://cloud.google.com/blog/topics/threat-intelligence/shinyhunters-targets-education-sector-oracle-exploit
- https://arcticwolf.com/resources/blog/critical-oracle-peoplesoft-vulnerability-actively-exploited-in-shinyhunters-campaign/
- https://ismalicious.com/posts/oracle-peoplesoft-zero-day-shinyhunters-data-theft

CVE-2026-20253 – SPLUNK ENTERPRISE (EJECUCIÓN REMOTA DE CÓDIGO PRE-AUTENTICADA VÍA ENDPOINT SIDECAR)

Se ha corregido una vulnerabilidad crítica en la plataforma de análisis de datos y SIEM Splunk Enterprise que permite a un atacante remoto no autenticado realizar operaciones arbitrarias de archivos y lograr la ejecución remota de código (RCE). El fallo radica en un componente complementario (sidecar) de PostgreSQL que carece por completo de controles de validación de identidad. Debido a que Splunk es el núcleo de visibilidad de los Centros de Operaciones de Seguridad (SOC) e ingesta registros altamente confidenciales de toda la infraestructura corporativa, un compromiso en este sistema representa un riesgo de control total del entorno de monitoreo.

Resumen técnico:

- Identificador principal: CVE-2026-20253 (Advisory ID: SVD-2026-0603).
- Severidad: Crítica (Puntaje base de 9.8 en CVSS v3.1).
- Causa raíz: Ausencia de controles de autenticación en una función crítica (CWE-306) localizada en el servicio sidecar de PostgreSQL utilizado en las instalaciones locales (On-Premises).
- Mecanismo de falla: Aunque el sidecar de PostgreSQL escucha localmente, la interfaz web principal de Splunk reenvía peticiones externas hacia sus endpoints de recuperación (/v1/postgres/recovery/backup y /restore). Un atacante puede evadir la autenticación enviando cabeceras HTTP Basic vacías. Mediante secuencias de salto de directorio (Path Traversal) en el parámetro del archivo de respaldo, se puede forzar al sistema a conectarse a una base de datos externa controlada por el atacante, descargar un volcado SQL malicioso, utilizar el archivo local de contraseñas .pgpass de Splunk para autorizarse localmente y ejecutar código SQL que sobrescribe scripts recurrentes de la aplicación.
- Estado de explotación: No se han reportado ataques activos en el entorno real al momento de su divulgación oficial, pero la firma de investigación watchTowr Labs publicó los detalles técnicos y la cadena completa del exploit el 12 de junio de 2026, lo que eleva drásticamente el riesgo de ataques oportunistas inminentes.
- Versiones afectadas: Splunk Enterprise en las ramas de mantenimiento 10.2.0 a 10.2.3, 10.0.0 a 10.0.6, 9.4.0 a 9.4.11 y 9.3.0 a 9.3.12. La infraestructura de Splunk Cloud Platform no se ve afectada debido a que no implementa este sidecar de soporte.

Impacto potencial:

- Ejecución de código arbitrario (RCE) antes de autenticación: Permite a un atacante remoto posicionarse dentro del sistema operativo subyacente con los privilegios de la cuenta de servicio de Splunk, sirviendo como un vector inmediato de acceso inicial a la red corporativa.
- Destrucción y truncamiento de archivos críticos del sistema: Al abusar de la primitiva de escritura, el atacante puede corromper, limpiar o sobrescribir archivos de configuración esenciales o bases de datos internas, provocando una denegación de servicio (DoS) permanente en la plataforma de monitoreo.
- Manipulación de trazas y ocultación de actividades maliciosas: Un atacante con control sobre el motor de indexación y los scripts de Splunk puede alterar los registros históricos de eventos, eliminar alertas de auditoría y cegar por completo al equipo de seguridad ante otras actividades maliciosas concurrentes en la red.
- Acceso a datos altamente confidenciales e infraestructura del SOC: Al comprometer la plataforma centralizadora de logs, el actor de amenazas obtiene acceso indirecto a la información técnica de servidores, credenciales expuestas en trazas de errores, arquitecturas de red y métricas operativas de toda la organización.

Recomendaciones de mitigación:

1. Actualización inmediata a las versiones corregidas por el fabricante: Se debe priorizar la actualización de los servidores Splunk Enterprise hacia las versiones parcheadas oficiales: 10.4.0, 10.2.4, 10.0.7, 9.4.12 o 9.3.13, dependiendo de la rama tecnológica en uso.
2. Aislamiento de red y endurecimiento de puertos de gestión: Restringir el acceso a los puertos de administración (como el puerto web de Splunk y el puerto de gestión 8089) mediante firewalls de red o reglas de control de acceso (ACL), permitiendo conexiones únicamente desde subnets administrativas confiables y prohibiendo la exposición directa a Internet.
3. Monitoreo preventivo de URIs y endpoints de recuperación: Configurar reglas de detección en el proxy inverso o en el firewall de aplicaciones web (WAF) para alertar o bloquear de inmediato llamadas anómalas dirigidas externamente hacia las rutas /v1/postgres/recovery/backup y /v1/postgres/recovery/restore.
4. Auditoría e inspección de integridad de scripts de Splunk: Implementar un control de integridad de archivos (FIM) sobre el directorio de aplicaciones de Splunk (especialmente en rutas como /opt/splunk/etc/apps/) para identificar de manera temprana modificaciones no autorizadas o inserciones de código malicioso en scripts de Python automatizados (como ssg_enable_modular_input.py).

Prioridad: Crítica.

Ampliar información:

- https://orca.security/resources/blog/cve-2026-20253-splunk-enterprise-rce-unauthenticated-file-operations/
- https://thehackernews.com/2026/06/critical-splunk-enterprise-flaw-lets.html
- https://unaaldia.hispasec.com/splunk-corrige-un-fallo-critico-en-splunk-enterprise-que-abre-la-puerta-a-ejecucion-remota-de-codigo-sin-autenticacion/
- https://www.picussecurity.com/resource/blog/splunk-cve-2026-20253-unauthenticated-remote-code-execution-vulnerability-explained
- https://oceanichost.com/blog/splunk-enterprise-cve-2026-20253-unauthenticated-rce-and-mitigation-paths

CVE-2026-48907 – JOOMLA JCE (EJECUCIÓN REMOTA DE CÓDIGO NO AUTENTICADA VÍA CONTROL DE ACCESO DEFECTUOSO)

Se ha emitido una alerta máxima por la explotación activa de una vulnerabilidad crítica que afecta a la extensión Joomla Content Editor (JCE), uno de los componentes de edición de texto y gestión de medios más utilizados en sitios web basados en el CMS Joomla. El fallo permite a atacantes remotos y completamente anónimos saltarse los controles de seguridad perimetrales, crear perfiles administrativos falsos y cargar archivos de ejecución PHP (web shells) para tomar el control absoluto del servidor host. Debido a la gravedad y la automatización de los ataques en el entorno real, la Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA) ha incorporado de manera urgente esta vulnerabilidad en su catálogo KEV.

Resumen técnico:

- Identificador principal: CVE-2026-48907.
- Severidad: Máxima / Crítica (Puntaje base de 10.0 en CVSS v3.1).
- Causa raíz: Control de acceso inapropiado (Improper Access Control) en la función de importación de perfiles de la extensión del editor.
- Mecanismo de falla: Un actor malicioso envía una solicitud HTTP POST malformada y dirigida de forma directa hacia el endpoint expuesto index.php?option=com_jce&task=profiles.import. Al carecer de una validación de sesión de nivel administrativo, el componente procesa la solicitud de un usuario no autenticado, permitiéndole forzar la creación de nuevos perfiles de edición permisivos. A través de este nuevo perfil, el atacante carga scripts PHP maliciosos directamente en directorios web públicos (como /images/ o /tmp/), los cuales se ejecutan de manera inmediata al ser invocados a través del navegador web, heredando los privilegios del proceso del servidor (ej. Apache, Nginx o PHP).
- Estado de explotación: Explotación activa masiva y automatizada en el entorno real mediante botnets globales que realizan escaneos oportunistas. Código de exploit de prueba de concepto (PoC) disponible públicamente. Incluido en el catálogo KEV de CISA el 16 de junio de 2026.
- Versiones afectadas: Todas las versiones de Joomla Content Editor (JCE) desde la 1.0.0 hasta la 2.9.99.4. El fallo fue subsanado en la versión 2.9.99.5 y blindado en la 2.9.99.6.

Impacto potencial:

- Ejecución remota de código (RCE) y control del sistema operativo: Concede a actores externos la capacidad de ejecutar comandos arbitrarios en el servidor web Linux/Windows subyacente, operando bajo el usuario del servicio web que posee acceso a los archivos de configuración y bases de datos.
- Establecimiento de persistencia mediante Web Shells: La carga exitosa de scripts PHP maliciosos en directorios con permisos de escritura proporciona una puerta trasera (backdoor) permanente para los atacantes, permitiéndoles mantener el acceso y manipular la infraestructura incluso si se bloquea el tráfico posterior.
- Envenenamiento de SEO institucional y desvío de tráfico: Campañas observadas asocian este compromiso con esquemas de monetización ilícita mediante redes de blogs privados (PBN), inyectando enlaces ocultos redirigidos a portales de apuestas o contenido adulto, lo que destruye el posicionamiento en buscadores (Google Search Console) y genera penalizaciones de reputación.
- Pivoteo de red interna y escalación de privilegios: El servidor web comprometido puede ser utilizado como una base de lanzamiento perimetral para escanear subredes internas adyacentes, buscar aplicaciones vulnerables y explotar configuraciones defectuosas para escalar privilegios a nivel de usuario root o Administrador del sistema.

Recomendaciones de mitigación:

1. Actualización mandatoria e inmediata de la extensión: Actualizar de manera prioritaria el plugin JCE a la versión 2.9.99.5 o superior e instalar las últimas actualizaciones de hardening del núcleo de Joomla. Nota: La actualización previene futuros ataques, pero no remueve web shells inyectadas previamente.
2. Auditoría forense de archivos y registros de acceso web: Inspeccionar los logs de Apache/Nginx ejecutando comandos de búsqueda (ej. grep "option=com_jce" | grep "task=profiles.import") para identificar peticiones POST anómalas. Asimismo, realizar un escaneo del sistema de archivos mediante instrucciones de consola como find /var/www/html -name "*.php" -mtime -3 para aislar archivos creados en las carpetas de carga de medios.
3. Restricción estricta de permisos de ejecución en directorios de medios: Modificar las directivas de configuración del servidor web (vía archivos .htaccess en Apache o bloques de ubicación en Nginx) para denegar de manera absoluta la ejecución de scripts PHP dentro de carpetas destinadas exclusivamente a imágenes y archivos estáticos (ej. /images/*).
4. Implementación de parches virtuales en el WAF corporativo: Configurar firmas personalizadas y reglas de bloqueo estricto en el Firewall de Aplicaciones Web (WAF) perimetral para interceptar y descartar inmediatamente cualquier petición entrante dirigida al componente vulnerable de JCE que provenga de direcciones IP externas no verificadas.

Prioridad: Crítica.

Ampliar información:

- https://saptanglabs.com/joomla-jce-vulnerability-why-unauthenticated-code-execution-demands-continuous-validation/
- https://thehackernews.com/2026/06/cisa-warns-of-actively-exploited-joomla.html
- https://linuxsecurity.com/news/security-vulnerabilities/critical-joomla-jce-rce-cisa-kev-linux-web-servers
- https://techjacksolutions.com/scc-vendor-rollup/widget-factory-joomla-jce-plugin-vulnerability-rollup-2026-06-17/
- https://securityaffairs.com/193775/hacking/u-s-cisa-adds-widget-factory-joomla-content-editor-jce-flaw-to-its-known-exploited-vulnerabilities-catalog.html

MALWARE

ROKAROLLA – TROYANO BANCARIO PARA ANDROID CON CAPACIDADES DE CONTROL TOTAL DE DISPOSITIVOS

Se ha identificado una variante altamente agresiva e invasiva de troyano bancario para sistemas operativos Android denominada "Rokarolla", nombrada así por la arquitectura de su infraestructura de comando y control (C2). Este malware destaca por ir más allá del simple robo de credenciales, consolidando una suite avanzada de toma de control administrativo total del dispositivo de la víctima. Distribuido de manera maliciosa mediante técnicas de ingeniería social fuera de la tienda oficial, abusa de los servicios nativos del sistema operativo para operar en absoluto silencio, neutralizar alertas y desviar fondos de manera invisible.

Resumen técnico:

- Tipo de amenaza: Troyano bancario móvil (Android Banking Trojan).
- Objetivos de la campaña: Monitoreo dinámico e inyección dirigida contra 217 aplicaciones financieras que incluyen plataformas de banca móvil, billeteras de criptomonedas y aplicaciones de redes sociales de alta frecuencia (como WhatsApp).
- Mecanismos de distribución: Difusión a través de portales web ilegítimos (como infocontablidades.it.com) que engañan a los usuarios mediante la descarga directa (sideloading) de archivos APK maliciosos que suplantan a Google Chrome o TikTok. El proceso inicia con un dropper primario que finge ser una actualización de seguridad de Google Play Protect.
- Mecanismo de comando y control (C2): Comunicación bidireccional cifrada sobre HTTPS que soporta una biblioteca operativa de 137 comandos remotos. Cuenta con una topología redundante basada en dominios de contingencia (fallback), identificándose en las trazas los servidores activos beralisvc.info, blestorians.cfd, abiorime.cfd y morevoms.cfd.
- Abuso de características del sistema: Explotación intensiva de los Servicios de Accesibilidad (Accessibility Services) de Android para leer las coordenadas y nodos de la interfaz gráfica, combinado con solicitudes fraudulentas para configurarse como la aplicación predeterminada para la gestión de llamadas y mensajes SMS.

Impacto potencial:

- Robo masivo de credenciales financieras mediante superposiciones dinámicas: Al abrir una de las 217 aplicaciones financieras monitorizadas, el malware inyecta de manera instantánea una interfaz falsa basada en HTML (Overlay Phishing) que se dibuja exactamente encima de la aplicación legítima, capturando nombres de usuario, contraseñas, números de tarjetas de crédito y enviándolos en tiempo real a los atacantes.
- Intercepción total de factores de autenticación (SMS y alertas): Al asumir el control de la mensajería y llamadas por defecto, Rokarolla intercepta de manera invisible las contraseñas de un solo uso (OTP) y tokens de doble factor (2FA) enviados por las entidades financieras. Adicionalmente, tiene la capacidad de bloquear llamadas telefónicas entrantes, impidiendo que los centros de prevención de fraude bancario se comuniquen con la víctima.
- Vigilancia de pantalla y registro de datos mediante "Pseudo-VNC": A diferencia del malware convencional que genera alertas visibles de transmisión, Rokarolla utiliza un mecanismo silencioso de capturas de pantalla secuenciales comprimidas en PNG que se envían con marcas de tiempo al C2. Esto opera en paralelo con un keylogger que extrae de manera transparente datos confidenciales de chats como WhatsApp y notificaciones generales.
- Evasión persistente y manipulación silenciosa del portapapeles: El troyano modifica los registros de texto del dispositivo sin intervención del usuario; si la víctima copia una dirección de billetera de criptomonedas para realizar una transferencia, el malware altera el portapapeles sustituyéndola por una dirección del atacante de forma imperceptible. Además, ejecuta comandos específicos para deshabilitar las protecciones nativas de Google Play Protect y suprimir el audio/vibración del teléfono para evitar sospechas.

Recomendaciones de mitigación:

1. Restricción estricta de la instalación de aplicaciones externas (Sideloading): Configurar y forzar de manera centralizada en los dispositivos corporativos la prohibición de instalación de aplicaciones provenientes de orígenes desconocidos, concientizando al personal para descargar software única y exclusivamente desde la tienda oficial Google Play Store.
2. Auditoría minuciosa y denegación de permisos de Accesibilidad: Monitorear activamente las solicitudes de permisos en los dispositivos de los usuarios. Ninguna aplicación convencional (navegadores, juegos o herramientas de redes sociales) debe recibir autorización para acceder a los "Servicios de Accesibilidad", "Acceso a Notificaciones" o el rol de "Manejador Predeterminado de SMS/Llamadas", ya que estas funciones otorgan control total sobre la UI.
3. Implementación de soluciones avanzadas de Mobile Threat Defense (MTD): Desplegar herramientas de seguridad móvil basadas en comportamiento y análisis heurístico en tiempo real (como Zimperium MTD o zDefend) que sean capaces de interceptar anomalías en la capa de la aplicación, detener procesos de sideloading táctico y bloquear el tráfico saliente hacia la infraestructura de red del C2 identificada.
4. Escrutinio riguroso de interfaces y flujos de autenticación: Educar a los usuarios finales para que desconfíen si una aplicación bancaria solicita prompts de autenticación repetidos, o si el dispositivo despliega pantallas persistentes de "Instalando actualización" que bloqueen la interacción ordinaria. Ante cualquier sospecha, se debe forzar el cierre de la app, desvincular el dispositivo de la red y realizar un análisis de compromiso o restauración de fábrica.

Prioridad: Urgente.

Ampliar información:

- https://zimperium.com/blog/rokarolla-android-banker-with-complete-device-takeover-capabilities
- https://www.malwarebytes.com/blog/mobile/2026/06/rokarolla-android-malware-can-take-over-your-phone-and-steal-banking-logins
- https://www.helpnetsecurity.com/2026/06/17/rokarolla-android-banking-trojan-device-takeover/
- https://www.govinfosecurity.com/rokarolla-android-banking-trojan-enables-device-takeover-a-31996
- https://securityaffairs.com/193745/cyber-crime/new-rokarolla-android-trojan-targets-217-banking-and-crypto-apps.html
- https://thehackernews.com/2026/06/new-rokarolla-android-malware-steals.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

FORTIBLEED: MÁS DE 73.000 FIREWALLS FORTINET COMPROMETIDOS EN CAMPAÑA GLOBAL DE RECOPILACIÓN DE CREDENCIALES

Se ha revelado una operación de ciberespionaje masiva y automatizada a escala industrial, denominada "FortiBleed", que ha dejado expuestas las credenciales de administración y accesos SSL VPN válidos de al menos 73.932 firewalls Fortinet únicos en 194 países. A diferencia de un incidente tradicional, esta campaña no explota una nueva vulnerabilidad de día cero (Zero-Day), sino que capitaliza la reutilización masiva de contraseñas previamente filtradas por malware de tipo infostealer, combinada con la alarmante ausencia de mecanismos de autenticación multifactor (MFA) en interfaces expuestas directamente a Internet. El incidente compromete de manera crítica el perímetro de más de 21.000 dominios corporativos globales, afectando a multinacionales, agencias gubernamentales e infraestructuras críticas.

Resumen técnico:

- Identificador principal: Campaña FortiBleed (Sin CVE asociado; no se trata de un fallo de software del producto).
- Severidad / Alcance: Alerta Máxima. De acuerdo con los análisis de red y telemetría de Shodan, la base de datos expuesta representa aproximadamente el 50% de la totalidad de firewalls Fortinet visibles e indexados en el internet global.
- Causa raíz e Higiene: Explotación de la reutilización de credenciales corporativas débiles o estáticas y fallas en la actualización del esquema de cifrado interno de los appliances. Aunque Fortinet introdujo un mecanismo de hashing robusto basado en PBKDF2 en actualizaciones recientes de FortiOS (7.2.11, 7.4.8 y 7.6.1) para reemplazar el almacenamiento débil SHA-256 con Salt, las contraseñas heredadas se mantienen desprotegidas en la base de datos oculta (old-password) hasta que cada administrador inicia sesión de forma manual tras la actualización.
- Mecanismo de ataque: Los atacantes ejecutaron una campaña masiva de password spraying a nivel industrial (registrando más de 1.160 millones de intentos de inicio de sesión contra objetivos FortiGate). De forma paralela, interceptaron de forma activa los hashes de autenticación SSL VPN almacenados en formatos SHA-256 antiguos y los descifraron fuera de línea (offline) utilizando un clúster dedicado de 45 GPUs orquestado mediante la herramienta de código abierto Hashtopolis. Una vez que recuperaban la contraseña en texto plano y validaban el acceso, el firewall comprometido se convertía en un punto de escucha pasivo para capturar nuevas credenciales y facilitar el movimiento lateral.
- Estado de la campaña: Campaña activa masiva documentada formalmente a mediados de junio de 2026 por investigadores independientes y firmas de inteligencia de amenazas (Hudson Rock, SOCRadar y el especialista Kevin Beaumont). Los vectores operativos y el perfilado detallado de las víctimas (ingresos, sector e industria) apuntan a un grupo cibercriminal altamente coordinado de habla rusa con motivaciones tanto financieras como geopolíticas (concentrando ataques en países de la OTAN).

Impacto potencial:

- Acceso remoto no autorizado y control total del perímetro: Al poseer las credenciales de administrador y VPN en texto plano, los actores de amenazas pueden evadir de forma legítima los firewalls perimetrales, permitiéndoles alterar de forma invisible las reglas de control de acceso, deshabilitar inspecciones de seguridad o sembrar usuarios de puerta trasera (backdoors).
- Movimiento lateral profundo hacia redes internas y Active Directory: Al consolidar el acceso a nivel de túnel de red a través de la VPN corporativa comprometida, los operadores dirigen sus ataques directamente contra los entornos internos de gestión de identidades corporativas (Active Directory), comprometiendo servidores de correo y bases de datos centrales.
- Espionaje pasivo y ciclo auto-alimentado de credenciales: Cada dispositivo comprometido actúa como una sonda maliciosa que monitoriza el tráfico de red transitado. El malware recolecta e indexa de forma continua nuevas contraseñas frescas que circulan por el firewall, enviándolas de regreso al servidor C2 de los atacantes para alimentar y expandir el ciclo de infección hacia otras empresas asociadas.
- Exfiltración de información clasificada e interrupción del negocio: La brecha del firewall perimetral facilita la sustracción de bases de datos y propiedad intelectual sensible. Los análisis forenses confirman intrusiones profundas en sectores de telecomunicaciones, salud, finanzas y la exfiltración exitosa de documentos clasificados pertenecientes a contratistas de defensa de la OTAN, dejando la infraestructura lista para posteriores campañas de ransomware.

Recomendaciones para mitigar el riesgo:

1. Forzar la rotación obligatoria y masiva de credenciales perimetrales: Restablecer de manera urgente todas las contraseñas asociadas con las interfaces de administración de FortiGate y perfiles de acceso de usuarios VPN corporativos. Debido a que las claves ya están filtradas en texto plano en las bases de datos criminales, la complejidad por sí sola de la contraseña actual no ofrece protección alguna.
2. Implementación universal y mandatoria de Autenticación Multifactor (MFA): Desplegar de forma estricta políticas de segundo factor de autenticación (MFA) en la totalidad de las pasarelas externas, conexiones SSL VPN y portales administrativos. Esta medida es la única que neutraliza de manera efectiva la efectividad de las credenciales robadas que circulan en texto plano.
3. Restricción y aislamiento de la interfaz gráfica de administración (Web UI): Aplicar políticas de acceso local (local-in policies) en FortiOS para asegurar que los paneles de gestión administrativa no estén expuestos directamente a la red pública de Internet, confinándolos exclusivamente a redes locales de administración internas (VLANs de gestión/O&M) o mediante accesos ZTNA.
4. Endurecimiento del algoritmo de hashing y eliminación de registros SHA-256: Tras elevar el firmware a las versiones protegidas de FortiOS, exigir que todos los administradores inicien sesión al menos una vez para forzar la conversión automática de sus credenciales al estándar seguro PBKDF2. Complementariamente, se recomienda habilitar la directiva login-lockout-upon-weaker-encryption en la política de contraseñas del sistema para purgar los hashes SHA-256 antiguos almacenados por compatibilidad.
5. Auditoría forense activa de sesiones y cuentas locales: Monitorear de forma exhaustiva los registros de acceso de los Security Gateways mediante comandos CLI (get vpn ssl monitor y show system admin) para identificar de manera temprana la creación de cuentas administrativas locales sospechosas, inicios de sesión desde ubicaciones geográficas anómalas o sesiones VPN activas inesperadas.

Prioridad: Urgente.

Ampliar Información:

- https://pasqualepillitteri.it/es/news/5280/fortibleed-credenciales-vpn-fortinet-robadas
- https://blog.segu-info.com.ar/2026/06/fortibleed-70000-firewall-fortinet.html?m=1
- https://www.diariobitcoin.com/noticias/fortibleed-expone-credenciales-vpn-de-fortinet-en-73-932-dispositivos-alrededor-del-mundo/
- https://arcticwolf.com/resources/blog/active-fortibleed-campaign-impacting-fortinet-devices-across-194-countries/
- https://blog.elhacker.net/2026/06/fortibleed-mas-de-70000-firewalls-de.html
- https://doublepulsar.com/fortibleed-75k-fortinet-firewalls-have-admin-passwords-cracked-60299faa65f8