



Boletín de Ciberseguridad Semanal

Edición °0626

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

BEYONDTRUST REMOTE SUPPORT Y PRA — EJECUCIÓN REMOTA DE CÓDIGO (RCE) PRE-AUTENTICACIÓN (CVE-2026-1731)

BeyondTrust ha emitido una alerta crítica tras corregir un fallo de seguridad que afecta a sus productos de Remote Support (RS) y Privileged Remote Access (PRA). La vulnerabilidad permite a un atacante remoto no autenticado ejecutar comandos en el sistema operativo con los privilegios del usuario del sitio, lo que representa un riesgo crítico de compromiso total.

Resumen técnico:

- Identificador principal: CVE-2026-1731 (Advisory BT26-02).
- Severidad: 9.9 (Crítica) en la escala CVSSv4.
- Causa raíz: Inyección de comandos del sistema operativo (CWE-78) debido a la neutralización inadecuada de elementos especiales en las solicitudes de los clientes.
- Mecanismo de falla: El atacante envía solicitudes web especialmente diseñadas (posiblemente a través de WebSockets) que el servidor procesa sin validar correctamente, permitiendo la ejecución de código antes de cualquier proceso de autenticación o interacción del usuario.
- Estado de explotación: No se ha reportado explotación activa en el mundo real hasta el momento, pero se han identificado aproximadamente 8,500 instancias on-premises expuestas en internet.
- Versiones afectadas: Remote Support 25.3.1 y anteriores; Privileged Remote Access 24.3.4 y anteriores.

Impacto potencial:

- Ejecución Remota de Código (RCE): Capacidad de tomar control total del servidor que gestiona el acceso remoto a la infraestructura crítica.
- Exfiltración de Datos: Acceso no autorizado a información sensible y registros de sesiones de soporte técnico.
- Interrupción del Servicio: Capacidad de inhabilitar las herramientas de soporte y administración remota de la organización.

Recomendaciones de mitigación:

1. Actualización Inmediata: Los clientes SaaS ya fueron parcheados automáticamente el 2 de febrero. Los clientes self-hosted deben migrar de forma manual a las versiones RS 25.3.2 y PRA 25.1.1 o superiores.
2. Aplicación de Parches Específicos: Instalar los paquetes BT26-02-RS o BT26-02-PRA según corresponda a la versión en uso.
3. Monitoreo de Logs: Revisar registros en busca de solicitudes malformadas o procesos inusuales originados por el usuario del sitio de BeyondTrust.

Prioridad: Crítica.

Ampliar información:

- <https://www.helpnetsecurity.com/2026/02/09/beyondtrust-remote-access-vulnerability-cve-2026-1731/>
- <https://horizon3.ai/attack-research/vulnerabilities/cve-2026-1731/>
- <https://www.rapid7.com/blog/post/etr-cve-2026-1731-critical-unauthenticated-remote-code-execution-rce-beyondtrust-remote-support-rs-privileged-remote-access-pra/>
- <https://www.beyondtrust.com/trust-center/security-advisories/bt26-02>
- <https://thehackernews.com/2026/02/beyondtrust-fixes-critical-pre-auth-rce.html>

FORTINET FORTICLIENTEMS – INYECCIÓN SQL CRÍTICA (CVE-2026-21643)

Fortinet ha emitido una alerta de seguridad crítica para su solución de gestión de endpoints, FortiClientEMS. Se ha identificado una vulnerabilidad de inyección SQL en la interfaz administrativa (GUI) que permite a un atacante remoto no autenticado ejecutar comandos u obtener acceso no autorizado al sistema mediante solicitudes HTTP diseñadas específicamente.

Resumen técnico:

- Identificador principal: CVE-2026-21643.
- Severidad: 9.8 - (Crítica).
- Causa raíz: Neutralización incorrecta de elementos especiales en comandos SQL (CWE-89) dentro del componente de la interfaz web.
- Mecanismo de falla: Un atacante puede enviar peticiones HTTP/HTTPS malintencionadas al servidor EMS. Al no validar adecuadamente las entradas, el sistema procesa estas peticiones como comandos de base de datos, lo que permite escalar a la ejecución de código en el servidor.
- Estado de explotación: No se ha detectado explotación activa en entornos reales al momento del reporte, pero debido al historial de ataques dirigidos contra Fortinet, el riesgo de ingeniería inversa del parche es alto.

- Versiones afectadas: Específicamente la versión 7.4.4 (rama 7.4). Las versiones 7.2, 8.0 y FortiEMS Cloud no se encuentran afectadas.

Impacto potencial:

- Ejecución de comandos remotos (RCE): Capacidad de ejecutar procesos no autorizados en el sistema operativo del servidor afectado.
- Compromiso total de la triada CID: Pérdida absoluta de confidencialidad, integridad y disponibilidad de la consola de administración de seguridad.
- Manipulación de políticas de seguridad: Posibilidad de alterar las configuraciones y políticas de protección desplegadas en todos los endpoints gestionados.
- Movimiento lateral y persistencia: El servidor EMS suele ser un punto de alta confianza en la red, lo que permite usarlo como base para comprometer otros sistemas internos o desplegar malware en cadena.

Recomendaciones de mitigación:

1. Actualización inmediata: Migrar de forma urgente a la versión FortiClientEMS 7.4.5 o versiones superiores que contienen el parche de seguridad.
2. Restricción de acceso administrativo: Limitar el acceso a la interfaz GUI de administración mediante segmentación de red, uso de VPN y listas de control de acceso (ACLs) por IP.
3. Auditoría de registros (Logs): Revisar exhaustivamente los registros de tráfico HTTP/HTTPS en busca de patrones de solicitudes anómalas dirigidas al puerto de gestión del EMS.
4. Aislamiento preventivo: En caso de no poder aplicar el parche de forma inmediata, desvincular la interfaz de gestión de cualquier exposición a redes públicas o segmentos de usuarios no confiables.

Prioridad: Crítica.

Ampliar información:

- <https://cibersafety.com/cve-2026-21643-inyeccion-sql-forticlientems/>
- <https://ciberseguridad.euskadi.eus/noticia/2026/vulnerabilidad-de-inyeccion-sql-sqli-en-la-interfaz-administrativa-que-afecta-a-forticlient-ems/webcyb00-contcibglos/es/>
- <https://thehackernews.com/2026/02/fortinet-patches-critical-sqli-flaw.html>
- <https://arcticwolf.com/resources/blog/cve-2026-21643/>
- <https://csirt.telconet.net/comunicacion/boletines-servicios/vulnerabilidad-critica-de-inyeccion-sql-en-forticlientems-para-fortinet/>

SAP CRM Y SAP S/4HANA – INYECCIÓN DE CÓDIGO CRÍTICA (CVE-2026-0488)

En el ciclo de actualizaciones de febrero de 2026, se ha identificado una vulnerabilidad de severidad máxima que afecta a las soluciones empresariales SAP CRM y SAP S/4HANA. El fallo permite que un atacante autenticado con privilegios mínimos ejecute sentencias SQL arbitrarias, lo que podría derivar en un compromiso total de la base de datos de la organización.

Resumen técnico:

- Identificador principal: CVE-2026-0488.
- Severidad: 9.9 (Crítica).
- Causa raíz: Falta de autorización y validación en las llamadas a módulos de funciones genéricas (CWE-862 / CWE-94).
- Mecanismo de falla: El fallo se localiza en el componente Scripting Editor. Un usuario autenticado puede manipular llamadas a módulos de funciones para saltarse las restricciones de seguridad y ejecutar comandos SQL directamente sobre la base de datos subyacente.
- Estado de explotación: No se ha reportado explotación activa en el mundo real ni se dispone de una prueba de concepto (PoC) pública hasta el 11 de febrero de 2026, pero la criticidad es máxima debido a la sensibilidad de los datos gestionados por SAP.

- Versiones afectadas: SAP CRM y SAP S/4HANA (específicamente instancias que utilicen el Scripting Editor).

Impacto potencial:

- Compromiso total de la base de datos: Capacidad para leer, modificar o eliminar cualquier registro almacenado en la base de datos del ERP/CRM.
- Escalada de privilegios: Un usuario con permisos limitados puede obtener control administrativo sobre los procesos de negocio críticos.
- Exfiltración de información sensible: Acceso no autorizado a datos financieros, de clientes, propiedad intelectual y registros de empleados.
- Interrupción de la continuidad del negocio: Posibilidad de causar denegación de servicio (DoS) o corrupción de datos que inhabilite las operaciones de la empresa.

Recomendaciones de mitigación:

1. Aplicación de la Nota de Seguridad SAP #3697099: Instalar de manera urgente los parches proporcionados por el fabricante en el Patch Day de febrero.
2. Restricción del Scripting Editor: Deshabilitar o limitar estrictamente el acceso al componente de edición de scripts únicamente al personal administrativo esencial.
3. Implementación del Principio de Mínimo Privilegio: Revisar y ajustar los roles de usuario y las configuraciones de UCON (Unified Connectivity) para evitar llamadas a funciones no autorizadas.
4. Monitoreo de Actividad de Base de Datos (DAM): Reforzar la auditoría de sentencias SQL ejecutadas desde los entornos CRM y S/4HANA para detectar patrones de inyección o consultas inusuales.

Prioridad: Crítica.

Ampliar información:

- <https://www.securityweek.com/sap-patches-critical-crm-s-4hana-netweaver-vulnerabilities/>
- <https://thehackernews.com/2026/02/over-60-software-vendors-issue-security.html>
- <https://cibersafety.com/cve-2026-0488-sap-crm-s4hana-inyeccion-codigo/>
- <https://feedly.com/cve/CVE-2026-0488>
- <https://www.heise.de/en/news/Patchday-SAP-CRM-S-4HANA-Attackers-can-damage-databases-11172823.html>

MALWARE

MALWARE – REYNOLDS RANSOMWARE CON TÉCNICA BYOVD (CVE-2025-68947)

Investigadores de ciberseguridad han detectado una nueva familia de ransomware denominada Reynolds, que destaca por integrar un componente BYOVD (Bring Your Own Vulnerable Driver) directamente en su carga útil. Esta técnica permite al malware deshabilitar soluciones de seguridad avanzadas (EDR/AV) antes de iniciar el cifrado, asegurando que sus actividades pasen desapercibidas para los sistemas de defensa.

Resumen técnico:

- Técnica principal: BYOVD (Abuso de controladores legítimos pero vulnerables para escalar privilegios y manipular el kernel).
- Controlador explotado: NSeckrnl.sys de la empresa NSecSoft (firmado digitalmente y legítimo).
- Vulnerabilidad asociada: CVE-2025-68947 (CVSS 5.7), que permite terminar procesos protegidos mediante solicitudes IOCTL malformadas.
- Estrategia de evasión: A diferencia de otros grupos que despliegan herramientas de evasión por separado, Reynolds incluye el driver dentro de su propio código, lo que reduce el ruido en la red y la probabilidad de detección temprana.

- Objetivos de desactivación: El malware está diseñado para finalizar procesos de Avast, CrowdStrike Falcon, Palo Alto Cortex XDR, Sophos, Symantec Endpoint Protection y Microsoft Defender, entre otros.

Impacto potencial:

- Cegado total de la defensa (EDR Blindness): Inhabilitación de las capacidades de detección y respuesta en los puntos finales, permitiendo que el ransomware actúe con total impunidad.
- Escalada de privilegios al Kernel: El uso del driver vulnerable permite al atacante ejecutar operaciones con privilegios de nivel SYSTEM, superando las protecciones estándar del sistema operativo.
- Cifrado irreversible de activos: Una vez desactivada la seguridad, el malware cifra los archivos locales con la extensión .locked, afectando la disponibilidad de la información.
- Persistencia mediante herramientas legítimas: Se ha observado el despliegue posterior de herramientas de acceso remoto como GoToHTTP, lo que sugiere que los atacantes buscan mantener el control incluso después del incidente.

Recomendaciones de mitigación:

1. Habilitar la lista de bloqueo de controladores de Microsoft: Asegurar que la función "Vulnerable Driver Blocklist" esté activa en Windows para impedir la carga de controladores conocidos como defectuosos.
2. Monitoreo de creación de servicios: Implementar reglas de detección para la creación inusual de servicios de sistema (especialmente aquellos que cargan drivers en modo kernel) y el uso de la herramienta sc.exe.
3. Fortalecimiento de la integridad del código (HVCI): Activar la integridad de código protegida por hipervisor para evitar que se carguen controladores no firmados o manipulados en el espacio de memoria del kernel.
4. Análisis de telemetría por comportamiento: Configurar alertas ante el cese repentino y coordinado de procesos de seguridad críticos, lo cual es un indicador claro de una fase previa de un ataque de ransomware.

Prioridad: Urgente.

Ampliar información:

- https://ciberconcienciadigital.com/noticia.php?blog_id=95&orden=2#google_vig_nette
- <https://securityaffairs.com/187869/security/reynolds-ransomware-uses-byovd-to-disable-security-before-encryption.html>
- <https://www.scworld.com/brief/byovd-technique-embedded-in-nascent-reynolds-ransomware>
- <https://thehackernews.com/2026/02/reynolds-ransomware-embeds-byovd-driver.html>
- <https://www.ciberplaneta.org/articles/745/>

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

FORTINET PUBLICA ACTUALIZACIONES CRÍTICAS ANTE VULNERABILIDADES DE ALTO IMPACTO EN FORTIOS Y FORTISANDBOX

Fortinet ha emitido una serie de avisos de seguridad que detallan múltiples vulnerabilidades críticas y de alta severidad que afectan a gran parte de su ecosistema, incluyendo FortiOS, FortiSandbox y FortiClientEMS. Los fallos corregidos abarcan desde omisiones de autenticación en servicios VPN hasta inyecciones SQL que permiten la ejecución remota de código (RCE). Esta ola de parches resalta la necesidad de una gestión de vulnerabilidades rigurosa y la actualización inmediata de los dispositivos de borde para prevenir intrusiones en redes corporativas.

Resumen técnico:

- Alcance de la amenaza: Los fallos identificados como CVE-2026-22153 (FortiOS) y CVE-2026-21643 (FortiClientEMS) representan los vectores de mayor riesgo. El primero permite eludir la autenticación LDAP en políticas de Agentless VPN y FSSO, mientras que el segundo facilita la ejecución de comandos arbitrarios mediante solicitudes HTTP malformadas.
- Componentes críticos afectados: El demonio fnbamd en FortiOS 7.6 y la interfaz administrativa de FortiSandbox se encuentran entre los puntos más vulnerables. Además, se reportaron fallos de Cross-Site Scripting (XSS) en FortiSandbox que podrían ser explotados sin necesidad de credenciales.
- Vectores de ataque: Los atacantes pueden aprovechar configuraciones específicas de servidores LDAP (como los unauthenticated binds) o injectar elementos especiales en comandos SQL para comprometer la tríada CID (Confidencialidad, Integridad y Disponibilidad) del sistema.
- Estado de explotación: Aunque hasta el 11 de febrero de 2026 no se han confirmado ataques masivos en el mundo real, la divulgación de estos fallos suele ir seguida de intentos de ingeniería inversa de los parches por parte de actores de amenazas.

Impacto potencial:

- Compromiso total de la seguridad perimetral: La capacidad de evadir la autenticación LDAP permite a usuarios no autorizados acceder a recursos críticos de la red interna protegidos por SSL-VPN.
- Ejecución remota de código (RCE): El control sobre el servidor de gestión (EMS) o el sandbox permite a un atacante instalar programas maliciosos, extraer configuraciones de firewall o crear cuentas con derechos de administrador total.
- Persistencia y movimiento lateral: Al vulnerar dispositivos de alta confianza como el FortiGate o el EMS, los atacantes obtienen una base sólida para pivotar hacia otros servidores de la organización.
- Fuga de información y manipulación de datos: Los fallos de inyección permiten la lectura o eliminación de registros sensibles de la base de datos de administración y la alteración de políticas de protección de endpoints.

Recomendaciones para mitigar el riesgo:

1. Actualización urgente de firmware: Migrar de inmediato a las versiones corregidas (FortiOS 7.6.5, FortiClientEMS 7.4.5 y FortiSandbox 5.0.2 o superiores) para cerrar los vectores de entrada conocidos.
2. Deshabilitar "Unauthenticated Binds" en LDAP: Para mitigar el bypass de autenticación, es crítico configurar el servidor LDAP (como Active Directory) para rechazar enlaces no autenticados, utilizando políticas de grupo o comandos de endurecimiento.
3. Restricción de acceso a interfaces de gestión: Aplicar políticas de acceso estricto a las interfaces GUI y portales VPN, limitando las conexiones únicamente a direcciones IP conocidas y mediante el uso obligatorio de autenticación multifactor (MFA).
4. Auditoría de logs y telemetría: Revisar registros de eventos en busca de solicitudes HTTP/HTTPS anómalas dirigidas a los puertos de gestión y monitorear la creación inusual de servicios o procesos en los dispositivos Fortinet.

Prioridad: Urgente.

Ampliar Información:

- <https://csirt.telconet.net/comunicacion/boletines-servicios/vulnerabilidad-de-omision-de-autenticacion-ldap-en-fortios/>
- https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-fortinet-products-could-allow-for-arbitrary-code-execution_2026-012
- <https://ciberseguridad.euskadi.eus/noticia/2026/vulnerabilidades-de-alto-impacto-en-productos-fortinet/webcyb00-contcibglos/es/>
- <https://www.cronup.com/feed-de-noticias-de-ciberseguridad-11-02-2026/>
- https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-fortinet-products-could-allow-for-arbitrary-code-execution_2026-012
- <https://www.fortiguard.com/psirt/FG-IR-25-1052>