# Boletín informativo
# Vulnerabilidad Microsoft Sharepoint

**CSIRTSALUD-AV-20260320-38**

**TLP: CLEAR**

| | |
|---|---|
| **Incidente ID:** | 038 |
| **Fecha del reporte:** | 20/03/2026 |
| **Entidad:** | Todas las Entidades del Ecosistema Digital |
| **Título:** | Explotación activa de vulnerabilidades en Microsoft Sharepoint |
| **Herramienta de detección** | N/A |
| **Activo involucrado:** | Microsoft |
| **Tipo de incidente:** | Boletín informativo |
| **Nivel de riesgo:** | Medio |

## Objetivo:

Informar a las entidades del Ecosistema y orientar a los equipos de ciberseguridad, administradores de red y gestores de riesgo sobre la existencia, naturaleza y riesgo de la vulnerabilidad **CVE-2026-20963**, identificada en Microsoft SharePoint Server.

Esta vulnerabilidad ha sido catalogada como **CRÍTICA (CVSS 9.8)** y se encuentra en explotación activa según la advertencia emitida por la Agencia de Ciberseguridad e Infraestructura de los Estados Unidos (CISA) el 18 de marzo de 2026, siendo incluida en el catálogo de Vulnerabilidades Explotadas Conocidas (KEV).

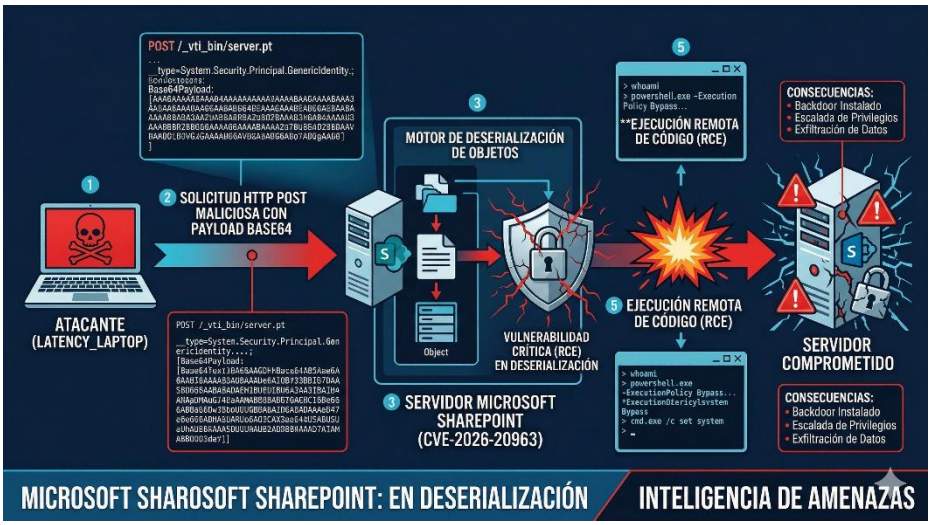

## Descripción:

CVE-2026-20963 es una vulnerabilidad de Ejecución Remota de Código (RCE) originada en la deserialización insegura de datos no confiables (CWE-502) dentro de Microsoft SharePoint Server. La falla reside en el procesamiento de objetos serializados a través de ASP.NET ViewState y otros flujos de datos serializados utilizados por las páginas de la aplicación SharePoint, típicamente ubicadas bajo el directorio /_layouts/.

# Boletín informativo
# Vulnerabilidad Microsoft Sharepoint

**CSIRTSALUD-AV-20260320-38** **TLP: CLEAR**

La serialización es el proceso mediante el cual una aplicación convierte estructuras de datos en un formato transportable (por red o almacenamiento). La deserialización es el proceso inverso: reconstruir el objeto original a partir de esos datos. Cuando esta operación no valida adecuadamente los datos de entrada, un atacante puede inyectar una carga maliciosa que al ser procesada ejecuta código arbitrario en el servidor.




Las características de la vulnerabilidad CVE-2026-20963 son las siguientes:

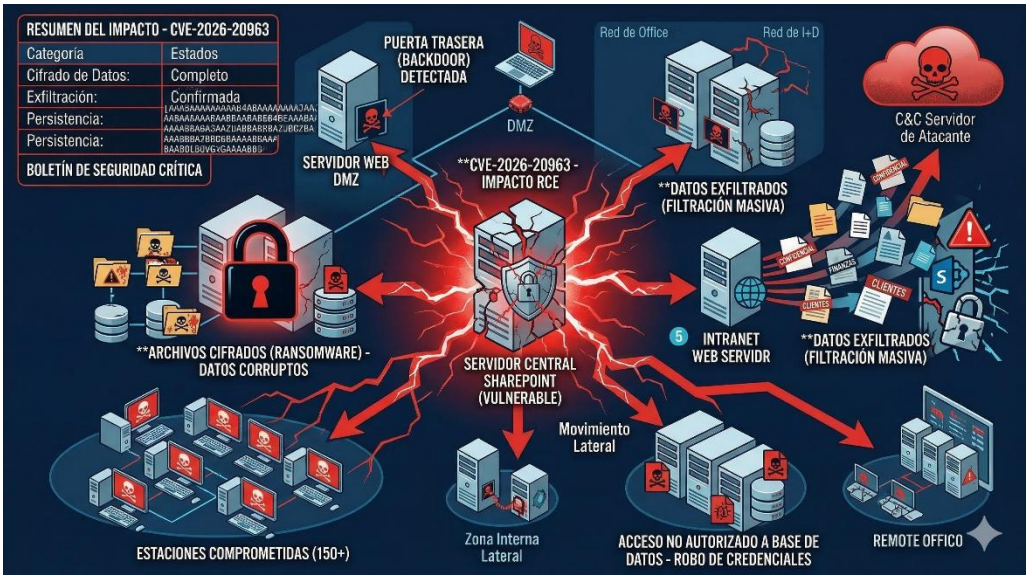
- **Clasificación:** CWE-502 — Deserialization of Untrusted Data
- **Vector de Ataque:** Red (Network-Based), sin interacción del usuario
- **Autenticación requerida:** Ninguna (ataque no autenticado)
- **Complejidad:** Baja
- **Impacto en Confidencialidad, Integridad y Disponibilidad:** COMPLETO (Alto)

La explotación exitosa de CVE-2026-20963 puede generar las siguientes consecuencias críticas:

| Consecuencia | Descripción |
|---|---|
| Ejecución de Código Remoto | Un atacante no autenticado puede ejecutar código arbitrario con los privilegios de la cuenta de servicio de SharePoint, obteniendo control total del servidor. |
| Compromiso Completo del Sistema | Si la cuenta de servicio de SharePoint tiene privilegios elevados, el atacante puede comprometer completamente el servidor. |
| Exfiltración de Datos | Acceso a documentos confidenciales, comunicaciones internas, credenciales y datos sensibles almacenados en SharePoint. |
| Movimiento Lateral | El servidor comprometido puede usarse como pivote para moverse a otros sistemas internos de la organización. |
| Despliegue de Backdoors | Instalación de shells web, implantes o puertas traseras para persistencia prolongada en la red. |
| Ransomware y Extorsión | Las vulnerabilidades RCE son el vector favorito de grupos ransomware para desplegar cargas de cifrado masivo. |
| Interrupción de Servicios | Posible caída o degradación del servicio de SharePoint afectando la continuidad operativa. |
| Incumplimiento Regulatorio | Exposición de datos puede derivar en sanciones por incumplimiento de normativas como GDPR, ISO 27001 o NIS2. |

# Boletín informativo
# Vulnerabilidad Microsoft Sharepoint

**CSIRTSALUD-AV-20260320-38** **TLP: CLEAR**




## Modo de explotación y cadena de infección

### Reconocimiento

El atacante realiza un reconocimiento previo para identificar servidores SharePoint expuestos y su versión:

- Escaneo de puertos (443, 80) para identificar instancias SharePoint públicamente accesibles.
- Fingerprinting de versión mediante cabeceras HTTP, páginas de error o rutas características.
- Verificación de la presencia del parámetro __VIEWSTATE en formularios de SharePoint.
- Uso de motores de búsqueda de activos como Shodan para identificar instancias sin parchear.

**Preparación del Payload**

El atacante utiliza herramientas especializadas para construir payloads de deserialización maliciosa:

- Herramienta principal: ysoserial.net, generador de gadget chains para deserialización .NET.
- Selección del gadget chain según las librerías presentes en el servidor objetivo (p.ej. TypeConfuseDelegate, WindowsIdentity, ActivitySurrogateSelector).
- El payload es una secuencia de clases y metodos que, al ser instanciados durante la deserialización, ejecutan comandos arbitrarios.
- El payload se codifica en Base64 para ser embebido en el parámetro __VIEWSTATE o __EVENTVALIDATION de una solicitud HTTP POST.

Ejemplo conceptual del flujo de construcción del payload:

```
ysoserial.exe -f BinaryFormatter -g TypeConfuseDelegate -c "cmd /c whoami > C:\\output.txt"
```

**Entrega del Payload (Explotación)**

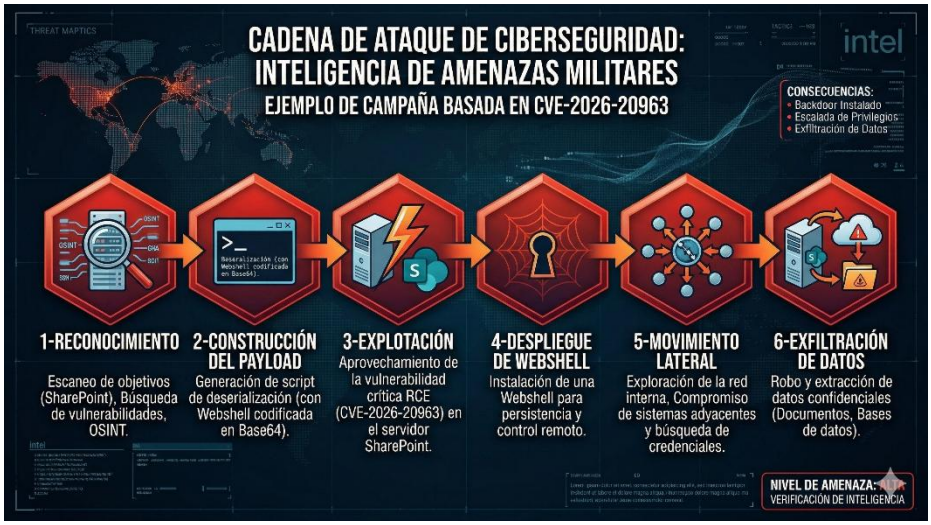
El payload malicioso es entregado al servidor mediante una solicitud HTTP POST:

- El atacante realiza una solicitud HTTP POST hacia una página vulnerable bajo /_layouts/ (p.ej. /_layouts/15/error.aspx, /_layouts/15/viewlsts.aspx).
- El parámetro __VIEWSTATE del body de la solicitud contiene el payload serializado codificado en Base64.
- El servidor SharePoint, al procesar la página, intenta deserializar el ViewState usando ObjectStateFormatter o BinaryFormatter.
- Al no existir validación de tipos, el formateador instancia el gadget chain malicioso.
- El gadget chain ejecuta el comando del atacante bajo el contexto de seguridad del proceso w3wp.exe (cuenta de servicio de SharePoint).

**Post-Explotación**

Tras obtener ejecución de código, el atacante escala su acceso:

- Despliegue de webshell: Escritura de un archivo .aspx malicioso en el directorio web de SharePoint para acceso persistente.
- Escalada de privilegios: Si la cuenta de servicio tiene privilegios de administrador local o de dominio, el atacante los aprovecha.
- Dumping de credenciales: Extracción de hashes NTLM o credenciales almacenadas mediante herramientas como Mimikatz.
- Movimiento lateral: Uso de credenciales robadas para pivotar hacia otros sistemas internos (Active Directory, servidores de archivos, bases de datos).
- Persistencia: Creación de tareas programadas, servicios maliciosos o modificación del registro de Windows.
- Exfiltración: Compresión y transferencia de datos sensibles hacia infraestructura del atacante.
- Preparación ransomware: Mapeo de recursos compartidos de red para despliegue masivo de ransomware.




## Relación con tácticas MITRE ATT&CK

La cadena de ataque asociada a CVE-2026-20963 se mapea con las siguientes tácticas y técnicas del framework MITRE ATT&CK:

| Táctica | Técnica / Sub-técnica | ID MITRE |
|---|---|---|
| Initial Access (Acceso Inicial) | Exploit Public-Facing Application | T1190 |
| Execution (Ejecución) | Exploitation for Client Execution / Server-Side Scripting | T1203 / T1059 |
| Persistence (Persistencia) | Server Software Component: Web Shell | T1505.003 |
| Persistence (Persistencia) | Scheduled Task/Job | T1053 |
| Privilege Escalation (Escalada) | Exploitation for Privilege Escalation | T1068 |
| Defense Evasion (Evasión) | Obfuscated Files or Information | T1027 |
| Credential Access (Credenciales) | OS Credential Dumping: LSASS Memory | T1003.001 |
| Discovery (Descubrimiento) | Network Service Discovery | T1046 |
| Lateral Movement (Movimiento Lateral) | Pass the Hash / Use Alternate Auth Material | T1550 |

| Táctica | Técnica / Sub-técnica | ID MITRE |
|---|---|---|
| Collection (Recolección) | Data from Information Repositories: SharePoint | T1213.002 |
| Exfiltration (Exfiltracion) | Exfiltration Over C2 Channel | T1041 |
| Impact (Impacto) | Data Encrypted for Impact (Ransomware) | T1486 |

**Descripción de las tácticas Clave**

- **T1190 — Exploit Public-Facing Application:** El atacante explota directamente la vulnerabilidad de deserialización en el servidor SharePoint expuesto a internet, sin necesidad de autenticacion previa.
- **T1505.003 — Web Shell:** Post-explotació+n, el atacante despliega una web shell (.aspx) en el directorio web de SharePoint para mantener acceso persistente y ejecutar comandos adicionales.
- **T1213.002 — Data from SharePoint**: SharePoint es una fuente primaria de datos sensibles. Los atacantes explotan el acceso para recopilar documentos confidenciales, emails y credenciales.
- **T1486 — Data Encrypted for Impact:** El acceso RCE en SharePoint puede usarse como punto de partida para desplegar ransomware en el entorno corporativo completo.

# Boletín informativo
# Vulnerabilidad Microsoft Sharepoint

**CSIRTSALUD-AV-20260320-38** **TLP: CLEAR**

## Activos o versiones afectados:

| Producto | Estado de Soporte | Acción Requerida |
|---|---|---|
| SharePoint Server Subscription Edition | Soporte Activo | **Aplicar KB5002685** |
| SharePoint Server 2019 | Soporte Activo | **Aplicar KB5002684** |
| SharePoint Enterprise Server 2016 | Soporte Activo | **Aplicar KB5002683** |
| SharePoint Server 2013 | **Fin de Soporte (EOL)** | **Actualizar a versión soportada** |
| SharePoint Server 2010 | **Fin de Soporte (EOL)** | **Actualizar a versión soportada** |
| SharePoint Server 2007 | **Fin de Soporte (EOL)** | **Actualizar a versión soportada** |

SharePoint Server 2007, 2010 y 2013 son versiones sin soporte (EOL). No recibirán actualizaciones de seguridad para esta ni futuras vulnerabilidades. Se requiere actualización **URGENTE** a una versión con soporte activo.

## Indicadores de compromiso:

Los siguientes indicadores deben ser monitoreados activamente en los sistemas SharePoint y su infraestructura adyacente:

**Indicadores en Registros de Acceso (Access Logs)**

- Solicitudes HTTP POST inusuales o anómalas hacia rutas bajo /_layouts/ con cuerpos de solicitud de gran tamaño.

- Peticiones POST repetidas con parámetros __VIEWSTATE o __EVENTVALIDATION con contenido codificado en Base64 extenso.
- Accesos desde IPs no reconocidas o desde rangos geográficos inesperados hacia endpoints de SharePoint.
- Solicitudes con User-Agents inusuales o automatizados (herramientas como curl, python-requests, ysoserial).
- Patrones de escaneo masivo contra múltiples rutas de /_layouts/ en cortos periodos de tiempo.

**Indicadores en el Sistema Operativo**

- Procesos hijos inusuales originados desde el proceso de SharePoint (w3wp.exe): cmd.exe, powershell.exe, net.exe, whoami.exe.
- Creación de archivos .aspx o .ashx nuevos en directorios web de SharePoint no esperados (webshells).
- Modificación de archivos de configuración de IIS o SharePoint.
- Ejecución de herramientas de descubrimiento de red (nmap, netstat, ipconfig) desde el contexto del proceso de SharePoint.
- Conexiones de red salientes no esperadas desde el servidor SharePoint hacia IPs externas (reverse shells).

**Indicadores en Logs de Eventos de Windows**

- Event ID 4688: Creación de procesos nuevos por w3wp.exe (proceso de IIS/SharePoint).
- Event ID 4624/4625: Intentos de autenticación fallidos masivos o exitosos desde IPs inusuales.
- Event ID 7045: Instalación de nuevos servicios no autorizados.
- Event ID 4698: Creación de nuevas tareas programadas.

- Event IDs de Sysmon 1, 3, 11: Creación de procesos, conexiones de red y creación de archivos sospechosos.

**Patrones de Payload (Firmas de Detección)**

- Presencia de gadget chains de ysoserial.net en solicitudes HTTP (patrones: AAEAAAD, TypeFilterLevel, System.Windows.Forms).
- Strings característicos en cuerpos de solicitudes: TypeConfuseDelegate, ActivitySurrogateSelector, TextFormattingRunProperties.
- Shells web con extensiones .aspx conteniendo eval(), base64_decode(), o Response.Write(Request[].

## Recomendaciones de mitigación:


**Aplicar el parche de seguridad de inmediato:**

- Descargar e instalar las actualizaciones de seguridad de enero 2026 desde el Microsoft Security Update Guide para la versión de SharePoint correspondiente. Esta es la acción más importante.
- Confirmar que todos los servidores SharePoint en el entorno han recibido el parche. Usar herramientas como WSUS, SCCM o inventario manual para asegurar cobertura total.
- Determinar qué instancias de SharePoint tienen exposición directa a internet e iniciar el parcheo por estas primero.
- Incrementar el nivel de logging en los servidores SharePoint y revisar los logs de los últimos 60 días en busca de indicadores de compromiso mencionados anteriormente.

**Cómo Mitigar si no es Posible Parchear Inmediatamente**

- Limitar el acceso al servidor SharePoint únicamente desde rangos IP confiables mediante firewall. Eliminar la exposición directa a internet si es posible.
- Desplegar o actualizar reglas del WAF para bloquear y detectar patrones conocidos de deserialización maliciosa en solicitudes HTTP POST hacia SharePoint.
- Revisar y deshabilitar características o APIs de SharePoint que procesen datos serializados y no sean estrictamente necesarias.
- Asegurarse de que la cuenta de servicio de SharePoint tenga los mínimos privilegios necesarios para operar, reduciendo el impacto de una explotación exitosa.
- Aislar el servidor SharePoint del resto de la red interna crítica para limitar el movimiento lateral en caso de compromiso.

**Cómo Detectar el Ataque**

Implementar las siguientes medidas de detección:

- Configurar alertas para solicitudes POST anómalas hacia /_layouts/ con parámetros de ViewState inusualmente grandes (>10KB).
- : Realizar búsquedas regulares de archivos .aspx o .ashx nuevos o modificados en directorios web de SharePoint.

- Implementar reglas en IDS/IPS para detectar payloads de deserialización .NET conocidos (cadenas como AAEAAAD, TypeConfuseDelegate).
- Ejecutar las siguientes consultas PowerShell en los servidores SharePoint:

```
# Buscar procesos hijos sospechosos de w3wp.exe
Get-WinEvent -FilterHashtable @{LogName='Security';Id=4688} | Where-Object
{$_.Message -like '*w3wp*'}
# Verificar webshells en directorio SharePoint
Get-ChildItem -Path 'C:\inetpub\wwwroot\wss' -Filter '*.aspx' -Recurse | Sort-Object
LastWriteTime | Select -Last 20
```

## Fuentes:


- **CISA — Known Exploited Vulnerabilities Catalog (KEV)** https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- **Microsoft Security Response Center (MSRC) — CVE-2026-20963** https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-20963
- **NIST National Vulnerability Database (NVD)** https://nvd.nist.gov/vuln/detail/CVE-2026-20963
- **MITRE ATT&CK Framework — Enterprise Matrix** https://attack.mitre.org
- **MITRE CWE-502 — Deserialization of Untrusted Data** https://cwe.mitre.org/data/definitions/502.html
- **Microsoft Update Catalog — KB5002685 / KB5002684 / KB5002683** https://www.catalog.update.microsoft.com
- **Microsoft Docs — SharePoint Server patching guide** https://learn.microsoft.com/en-us/sharepoint/install/install-for-sharepoint-server
- **BleepingComputer** — *"Critical Microsoft SharePoint flaw now exploited in attacks" Publicado: 19 de marzo de 2026*

https://www.bleepingcomputer.com/news/microsoft/critical-microsoft-sharepoint-flaw-now-exploited-in-attacks/

- **SecurityWeek** — *"CISA Warns of Attacks Exploiting Recent SharePoint Vulnerability" Publicado: 19 de marzo de 2026* https://www.securityweek.com/cisa-warns-of-attacks-exploiting-recent-sharepoint-vulnerability/
- **Help Net Security** — *"CISA warns of active exploitation of Microsoft SharePoint vulnerability (CVE-2026-20963)" Publicado: 19 de marzo de 2026* https://www.helpnetsecurity.com/2026/03/19/sharepoint-vulnerability-cve-2026-20963-exploited/
- **The Register** — *"Unknown attackers exploit another critical SharePoint bug" Publicado: 19 de marzo de 2026* https://www.theregister.com/2026/03/19/unknown_attackers_exploit_yet_another/
- **CyberSecurityNews** — *"Microsoft SharePoint Vulnerability Exploited in Attacks" Publicado: 19 de marzo de 2026* https://cybersecuritynews.com/microsoft-sharepoint-vulnerability-exploited/

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el CSIRT Salud a través de las líneas telefónicas (+57) 316 8931490 - 3181553570 o mediante el correo electrónico csirtsalud@minsalud.gov.co. Nuestro equipo está disponible para brindar el acompañamiento necesario.