Incidente ID:	0009
Fecha del reporte:	28/10/2025
Entidad:	Todas las Entidades del Ecosistema Digital
Título:	Ejecución remota de código de Microsoft WSUS (CVE-2025-59287) explotada activamente
Herramienta de detección	N/A
Activo involucrado:	Microsoft Windows Server
Tipo de incidente:	Boletín informativo
Nivel de riesgo:	Alto

Objetivo:

Informar a las entidades del ecosistema Digital sobre la vulnerabilidad de ejecución remota crítica en Windows Server Update Services (WSUS) con número CVE-2025-59287 y con una calificación de CVSS de 9.8

Descripción:

El 14 de octubre de 2025 se descubrió una vulnerabilidad crítica de ejecución remota de código (RCE) no autenticada en Windows Server Update Services (WSUS) de Microsoft, un componente esencial en la administración corporativa de parches. El parche inicial emitido por Microsoft durante el Martes de Parches de octubre no mitigó completamente la falla, lo que hizo necesaria la publicación de una actualización de seguridad de emergencia fuera de ciclo el 23 de octubre de 2025.

Pocas horas después de esta actualización, Unit 42 y otros equipos de investigación en ciberseguridad detectaron explotaciones activas de la vulnerabilidad en entornos reales. La conjunción de una vulnerabilidad RCE no autenticada y remotamente explotable en un servicio de infraestructura crítica, junto con evidencias de explotación activa, constituye una amenaza severa y de carácter urgente para las entidades que conforman el Ecosistema Digital.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Detalles de la vulnerabilidad:

Impacto: permite que un atacante remoto no autenticado ejecute código arbitrario con privilegios del sistema en los servidores afectados.

Estado: Explotado activamente. Se observó que actores de amenazas explotaban la vulnerabilidad pocas horas después de que Microsoft publicara un parche de emergencia el 23 de octubre.

Urgencia: La Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA) agregó esta vulnerabilidad a su Catálogo de Vulnerabilidades Explotadas Conocidas (KEV) el 24 de octubre, lo que subraya el riesgo inmediato.

Vector de ataque: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

Productos afectados:

Microsoft Windows Server en las siguientes versiones

- 2012
- 2012 R2
- 2016
- 2019
- 2022 (incluye la versión edición 23H2)
- 2025

Se debe tener en cuenta que la vulnerabilidad únicamente afecta a los servidores en los que se encuentra habilitado el rol de servidor WSUS. Esta función no se habilita de forma predeterminada durante la instalación del sistema operativo, por lo que es importante verificar en qué servidores se encuentra activa.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Modo de explotación de la vulnerabilidad

El modo de explotación de la vulnerabilidad cuenta con 4 etapas principales las cuales se describen a continuación.

1. Acceso inicial: los atacantes apuntan a instancias de WSUS expuestas públicamente en sus puertos TCP predeterminados, 8530 (HTTP) y 8531 (HTTPS).

2. Ejecución: Los comandos maliciosos de PowerShell se ejecutan mediante procesos principales específicos. Las cadenas de procesos forenses observadas durante las pruebas incluyen wsusservice.exe → cmd.exe → cmd.exe → powershell.exe y w3wp.exe → cmd.exe → cmd.exe → powershell.exe.

3. Reconocimiento: La carga útil inicial ejecuta comandos para recopilar información sobre el entorno de red interno, incluyendo whoami , net user /domain e ipconfig /all . Este conjunto de comandos inicial está diseñado para mapear rápidamente la estructura del dominio interno e identificar cuentas de usuario importantes, lo que proporciona al atacante un plan inmediato para el movimiento lateral.

4. Exfiltración de datos: la información recopilada se exfiltra a un punto final Webhook.site remoto controlado por el atacante mediante una carga útil de PowerShell que intenta Invoke-WebRequest y recurre a curl.exe si es necesario.

Indicadores de Compromiso

A continuación, se presenta el dominio relacionado con la vulnerabilidad, el dominio se encuentra ofuscado para evitar algún error que permita abrir el enlace relacionado.

Dominio
hxxp://webhook[.]sitio/22b6b8c8-2e07-4878-a681-b772e569aa6a

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Recomendaciones de mitigación:

Se debe aplicar de manera inmediata el parche de seguridad lanzado por Microsoft el 23 de octubre del 2025.

A continuación, se proporciona el enlace de la guía de instalación del parche de seguridad para cada una de las versiones afectadas.

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-59287

Pasos a seguir para la aplicación correcta del parche de seguridad de Microsoft

1 Seleccionar la versión de sistema operativo Windows Server que se tiene instalada y realizar la descarga desde el enlace proporcionado anteriormente.

2 Realizar la instalación del parche de seguridad

3 Una vez instalado el parche de seguridad se debe proceder con el reinicio del servidor

4 Hasta que el parche esté completamente desplegado y los servidores seguros, no eliminar (o dar por revertidas) las mitigaciones (bloqueos o deshabilitación) hasta haber confirmado la corrección.

5 Revisar y aplicar buenas prácticas de higiene de seguridad, como segmentación de red, gestión de roles/exposición, y asegurarse de que servicios internos no estén expuestos innecesariamente.

Si no se puede instalar el parche de seguridad se recomienda realizar las siguientes acciones para mitigar la vulnerabilidad.

- Priorizar la identificación de todos los servidores que tienen habilitado el rol WSUS (porque sólo estos están afectados) y determinar su estado de parcheo.
- Deshabilitar el rol de servidor WSUS en los servidores afectados.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

- Bloquear el tráfico entrante hacia los puertos TCP 8530 y 8531 (host firewall) en los servidores que tienen habilitado WSUS.
- Verificar que los servidores con el rol WSUS habilitado no estén expuestos a Internet (o que sólo lo estén con controles adecuados).
- Monitorear actividad inusual en el servidor WSUS (procesos inesperados, tráfico saliente extraño, puertos 8530/8531 abiertos hacia el exterior).

Fuentes:

- https://unit42.paloaltonetworks.com/microsoft-cve-2025-59287/
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-59287

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.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570