Grave vulnerabilidad en IIS. De vuelta a fallos de principios de década

Desde hace unos días, estamos viviendo una especie de desafortunada vuelta a principios de esta década por culpa de un grave fallo de seguridad en Internet Information Server, el servidor web de Microsoft. Se ha descubierto una vulnerabilidad «como las de antes» y, lo peor, aprovechando fallos y problemas que parecían pertenecer ya al pasado, como de otro tiempo. Al parecer, el fallo está disparando el número de «desfiguraciones» (defaces) en servidores web con IIS en los últimos días.

A cualquiera que esté al tanto de las noticias sobre seguridad le sonará que las palabras IIS, WebDAV, unicode y la cabecera «Translate:f» (parte del protocolo WebDAV) son términos que juntos, no han traído nunca nada bueno al servidor de Microsoft en los últimos años. La vulnerabilidad que acaba de ser descubierta combina todos esos elementos. Se ha encontrado un fallo en IIS 6.x a la hora de procesar peticiones http especialmente manipuladas con la cabecera «Translate:f» y con caracteres Unicode. Esto puede permitir a un atacante eludir la autenticación (y subir ficheros si lo permiten los permisos) al disparar un problema de validación en WebDAV.

Antecedentes (1999)

> *https://servidor.iis.afectado/ejemplo.asp.*
>
> *https://www.direccion.com/code/ejemplo.asp0x2e*

Antecedentes (2000)
[crayon-6a9d580abe29b749403057/]
Antecedentes (2001)

https://servidor.iis.afectado/scripts/../../../winnt/system32/cmd.exe?/c+dir+c:

https://servidor.iis.afectado/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir+c:

Antecedentes (2003): WebDAV

Y en 2009…
[crayon-6a9d580abe2a1343673758/]

Fuente

https://www.hispasec.com/unaaldia/3858