BOLETÍN DE ALERTA

Boletín Nro.: 2022-50
Fecha de publicación: 30/11/2022
Tema: Explotación activa de vulnerabilidad *RCE* que afecta a Windows IKE

Los productos afectados son:

- Windows server 2008, versión r2.
- Windows server 2012, versión r2.
- Windows 10, versiones 1607, 20h2, 21h1, 21h2 y 1809.
- Windows 8.1.
- Windows server 2016.
- Windows 7.
- Windows RT 8.1
- Windows 11.
- Windows server 2019.
- Windows server 2022.

Descripción:

Recientemente se han reportado incidentes de seguridad sobre una vulnerabilidad crítica reportada en las actualizaciones de seguridad de Microsoft del mes de septiembre, que afecta a los sistemas Microsoft Windows y que se está explotando activamente. La misma corresponde a una vulnerabilidad que afecta a Windows IKE (*Windows Internet Key Exchange*), que permitiría a un atacante realizar ejecución remota de código (*RCE*) en el sistema afectado. Actualmente para esta vulnerabilidad existe un PoC publicado en Internet.

La vulnerabilidad identificada como CVE-2022-34721, de severidad “Crítica” y con puntuación asignada de 9.8. Esta vulnerabilidad explotada activamente se debe a una falla en el protocolo de intercambio de claves de Internet (*IKE*) de Windows. Un atacante podría aprovechar esta vulnerabilidad para realizar ejecución remota de código (*RCE*) en el sistema, enviando un paquete especialmente diseñado a un nodo de Windows donde *IPSec* esté habilitado. Esta vulnerabilidad solo afecta a *IKEv1*.

Impacto:

La explotación exitosa de esta vulnerabilidad permitiría a un atacante ejecutar código de forma remota.

Solución:

Recomendamos acceder a la actualización de seguridad correspondiente al mes de septiembre, a través de la siguiente guía provista por Microsoft:

- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-34721

Adicionalmente, como medida de prevención recomendamos ejecutar cualquiera de los siguientes comandos para comprobar el estado de ejecución del servicio:

1. Power Shell:

```
C:\&gt; Get-Service Ikeext
```

2. Cmd:

```
C:\&gt; sc query ikeext
```

NOTA: Solo los sistemas con los módulos de claves *IKE* y *AuthIP IPsec* en ejecución son vulnerables a este ataque.

Información adicional:

- https://www.cert.gov.py/noticias/actualizaciones-de-seguridad-de-microsoft/
- https://securityonline.info/cybersecurity-firm-warns-of-actively-exploited-windows-ike-rce-cve-2022-34721-flaw/
- https://nvd.nist.gov/vuln/detail/CVE-2022-34721
- https://www.cyfirma.com/outofband/windows-internet-key-exchange-ike-remote-code-execution-vulnerability-analysis/
- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-34721