BOLETÍN DE ALERTA

Boletín Nro.: 2022-23
Fecha de publicación: 12/05/2022
Tema: Vulnerabilidades críticas en productos Microsoft.

Productos afectados:

- Microsoft Visual Studio, 2017, 2019, 2022.
- Microsoft Office y sus componentes.
- Microsoft .NET Framework, versiones anteriores a 4.8.
- Microsoft Windows RT8.1, 8.1, 7.
- Microsoft Windows Server, versiones 2008, 2008 R2, 2012, 2012 R2, 2016, 2019, 2022, 20H2.

Descripción:

Microsoft ha lanzado actualizaciones de seguridad, en un anuncio oficial del mes de mayo que subsanan un total de 75 vulnerabilidades, incluidas 3 de día cero. Las vulnerabilidades reportadas se componen de 7 (siete) de severidad "Crítica", 67 (sesenta y siete) de severidad "Alta" y 1 (uno) de severidad "Baja". Las principales se detallan a continuación:

- CVE-2022-26925 (Vulnerabilidad de falsificación de Windows LSA), vulnerabilidad de día cero, de severidad crítica que está siendo explotada activamente. La misma corresponde a una vulnerabilidad de suplantación de identidad en el *LSA* (local security authority) de Windows. Un atacante no autenticado podría obligar a los controladores de dominio a autenticarse en un servidor controlador del atacante mediante *NTLM.*

- CVE-2022-26937 (Vulnerabilidad de ejecución remota de código del sistema de archivos de red de Windows), de severidad crítica, con una puntuación de 9.8. Esta se debe a un error desconocido que afecta al sistema de archivo de red de Windows (*NFS*). Esto permitiría a un atacante realizar ejecución remota de código (*RCE*) del sistema de archivos de red de Windows.

- CVE-2022-29972 (Vulnerabilidad inyección de argumentos del controlador *Redshift*), de severidad crítica. Esta se debe a un error de autenticación basada en navegador del controlador *ODBC* de Amazon Redshift de Magnitude Simba. Esto permitiría a un atacante realizar ejecución remota de código (*RCE*).

- CVE-2022-22017 (Vulnerabilidad de ejecución remota de código en el cliente de Escritorio remoto), de severidad crítica. Esta se debe a un error en la conexión RDP. Esto permitiría a un atacante realizar ejecución remota de código (*RCE*) en el sistema de la víctima.

- CVE-2022-26923 (Vulnerabilidad de elevación de privilegios en los Servicios de dominio de *Active Directory*), de severidad crítica. Esta se debe a un posible fallo en servicio de dominio de *Active Directory*. Un atacante podría manipular atributos en cuentas de equipo que posee o administra y adquirir un certificado de Servicios de Active Directory realizando escalamiento de privilegios.

- CVE-2022-22012 y CVE-2022-29130 (Vulnerabilidades de ejecución remota de código LDAP de Windows), de severidad crítica, con una puntuación de 9.8. Una función desconocida del componente LDAP es afectada por esta vulnerabilidad. Estas vulnerabilidades pueden ser explotadas por un atacante autenticado en caso de que la política *LDAP* "*MaxReceiveBuffer*" se encuentre configurada en un valor más alto que el valor predeterminado (es decir, una mayor cantidad máxima de subprocesos que las solicitudes *LDAP* pueden contener por procesador).

Se puede acceder al listado completo de las vulnerabilidades aquí.

Impacto:

La explotación de estas vulnerabilidades permitiría a un atacante realizar ejecución remota de código (*RCE*), acceder a los controladores de dominio, escalamiento de privilegio, entre otros.

Mitigación:

Se recomienda instalar las actualizaciones correspondientes provistas por Microsoft, o bien, seguir las instrucciones para mitigar el riesgo asociado a cada CVE en el siguiente enlace:

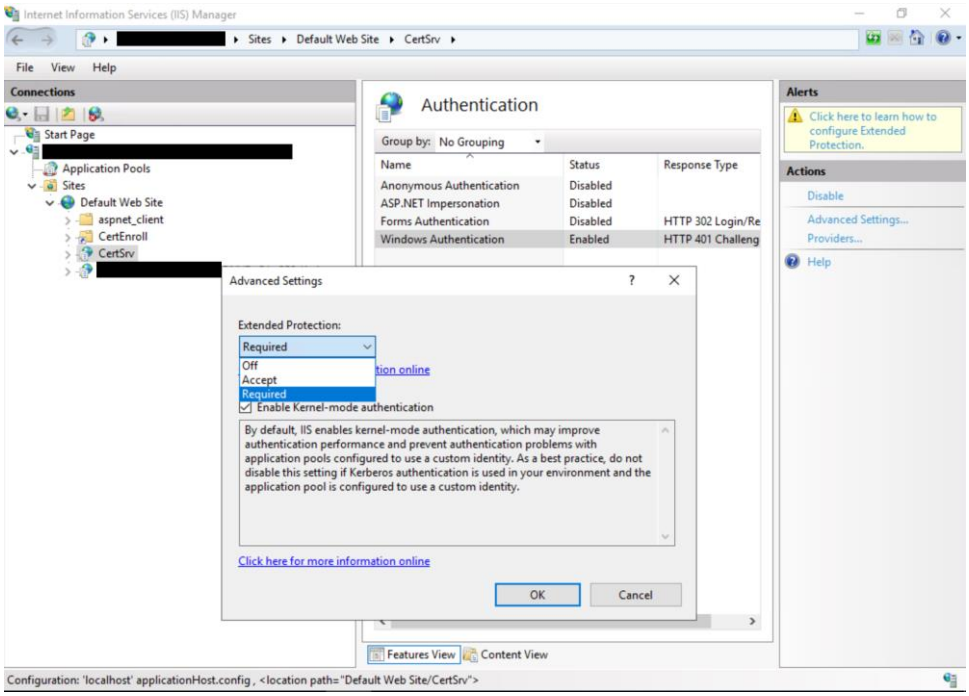
- https://msrc.microsoft.com/update-guide/releaseNote/2022-May

Adicionalmente, sugerimos seguir las siguientes instrucciones como mitigación para las vulnerabilidades CVE-2022-26925 y CVE-2022-26937:

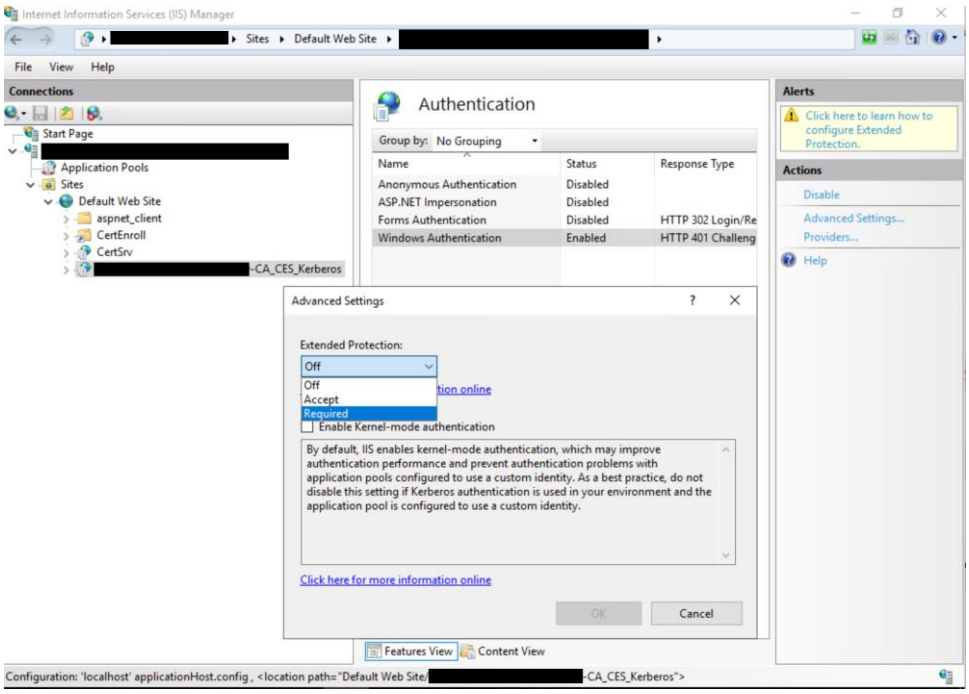
CVE-2022-26925 (Vulnerabilidad de falsificación de Windows LSA)

- Recomendamos habilitar *EPA* y deshabilitar *HTTP* en servidores *AD CS*. Abrir el Administrador de *Internet Information Services* (IIS):

1. Habilitar EPA para la inscripción web de la autoridad de certificación, siendo **Obligatorio** la opción más segura y recomendada:

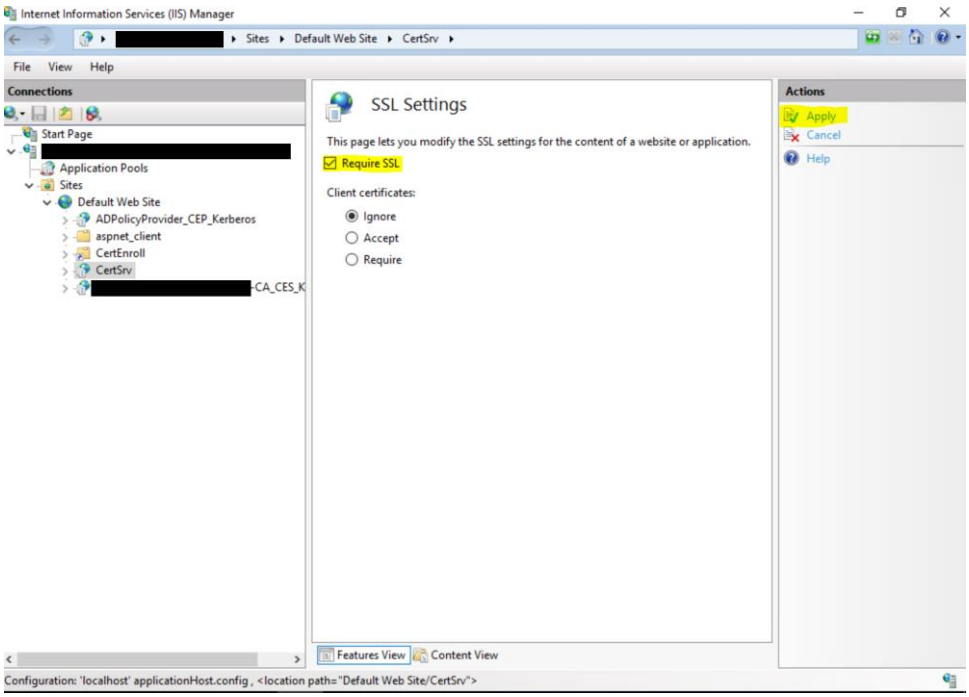


2. Habilitar EPA para el servicio web de inscripción de certificados, siendo Obligatorio la opción más segura y recomendada:



3. Luego de habilitar *EPA* en la interfaz de usuario, el archivo *Web.config* creado por el rol de CES en ***<%windir%>\systemdata\CES\<CAName>_CES_Kerberos\web.config*** también debe actualizar agregando ***<extendedProtectionPolicy>*** establecido con un valor de ***WhenSupported*** o ***Always*** , según la opción de ***Extended Protection*** seleccionada en la interfaz de usuario de IIS anterior.

4. Habilitar ***Requerir SSL*** , que habilitará solo las conexiones **HTTPS**.



Importante: Después de completar los pasos anteriores, deberá reiniciar el servidor IIS para cargar los cambios.

Fuente: https://support.microsoft.com/en-us/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429

CVE-2022-26937 (Vulnerabilidad de ejecución remota de código del sistema de archivos de red de Windows)

- Esta vulnerabilidad no se puede explotar en *NFSV4.1*. Antes de actualizar su versión de Windows que protege contra esta vulnerabilidad, puede mitigar el ataque al deshabilitar *NFSV2 y NFSV3*.

1. El siguiente comando de PowerShell deshabilitará esas versiones:

```
PS C:\Set-NfsServerConfiguration -EnableNFSV2 $false -EnableNFSV3 $false
```

2. Reiniciar el servidor NFS

```
nfsadmin server stop

nfsadmin server start
```

3. Para confirmar que NFSv2 y NFSv3 se han desactivado "*False*", ejecute el siguiente comando en una ventana de Powershell:

```
PS C:\Get-NfsServerConfiguration
```

Fuente: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-26937

Información adicional:

- https://portal.cci-entel.cl/Threat_Intelligence/Boletines/1243/
- https://threatpost.com/microsoft-zero-day-mays-patch-tuesday/179579/
- https://www.bleepingcomputer.com/news/microsoft/microsoft-may-2022-patch-tuesday-fixes-3-zero-days-75-flaws/

- https://msrc.microsoft.com/update-guide/releaseNote/2022-May