Advertencia de Seguridad

Importancia de la actualización de IIS en sitios Web

COLCERT AD-0810-023

El servidor web Internet Information Services (IIS) de Microsoft es ampliamente utilizado para alojar aplicaciones y sitios web. Sin embargo, como cualquier software, IIS está expuesto a vulnerabilidades que pueden ser explotadas por atacantes si no se mantiene actualizado. Este documento proporciona una guía sobre las mejores prácticas de seguridad para la gestión de IIS y resalta la importancia de realizar actualizaciones regulares para proteger los activos digitales y reducir el riesgo de ataques.

Riesgos al no tener actualizado IIS

Exposición a Vulnerabilidades Conocidas (CVE)

- **CVE-2017-7269:** Vulnerabilidad de Ejecución Remota de Código (RCE) a través de un desbordamiento de búfer en el servicio WebDAV, lo que permite a un atacante ejecutar comandos arbitrarios y tomar el control del servidor.
- **CVE-2021-31166:** Vulnerabilidad en HTTP.sys que permite la ejecución remota de código sin necesidad de autenticación.
- **CVE-2022-21907:** Vulnerabilidad que habilita un Ataque de Denegación de Servicio (DoS), lo que afecta la disponibilidad del servidor y puede causar interrupciones en las aplicaciones que dependen de él.
- **CVE-2020-0609 y CVE-2020-0610:** Fallos en la Puerta de Enlace de Escritorio Remoto (RD Gateway), que pueden utilizarse para obtener acceso no autorizado o ejecutar código malicioso en servidores IIS.

Explotación de Ataques Comunes

- **Inyección SQL:** Aunque es un ataque más común en las aplicaciones web, un IIS mal configurado puede facilitar este tipo de ataques si las defensas no están actualizadas.
- **Cross-Site Scripting (XSS):** Configuraciones incorrectas pueden permitir la ejecución de scripts maliciosos en el navegador de los usuarios, comprometiendo la información sensible.
- **Ataques MITM (Man-in-the-Middle):** Sin el uso de HTTPS y con protocolos desactualizados como TLS 1.0 o SSL 3.0, el servidor es susceptible a ataques de intermediarios, exponiendo la comunicación entre usuarios y el servidor.

Mayor Superficie de Ataque

- **Protocolos no seguros:** Un IIS sin actualizar puede utilizar versiones vulnerables de protocolos, como TLS 1.0 o SSL 3.0, que son susceptibles a ataques como POODLE o BEAST, permitiendo que los atacantes intercepten o modifiquen la comunicación.
- **Módulos innecesarios:** IIS desactualizado puede incluir módulos obsoletos como WebDAV o CGI, que han sido históricamente vulnerables y explotados en múltiples ataques, como CVE-2017-7269.

Fuente: https://cve.mitre.org

Ataques Conocidos Asociados a Vulnerabilidades de IIS

Ransomware: Vulnerabilidades como CVE-2017-7269 han sido aprovechadas para comprometer servidores y desplegar ransomware, lo que puede llevar al cifrado de datos críticos, exigiendo un rescate por su liberación.

Fuerza Bruta: Servidores mal configurados o sin actualizaciones pueden ser objetivo de ataques de fuerza bruta para comprometer cuentas administrativas y ganar acceso no autorizado.

Exploits Zero-Day: Las vulnerabilidades no parcheadas en IIS pueden ser explotadas mediante ataques de día cero, antes de que existan parches públicos disponibles.

COLCERT

Advertencia de Seguridad

Importancia de la Actualización de IIS en sitios Web

COLCERT AD-0810-023

Medidas de mitigación:

Se recomienda actualizar a las versiones más recientes:

- ✓ Versión estable: IIS 10.0 (incluida en Windows Server 2016, 2019 y 2022).
- ✓ Versión principal: IIS 10.0 (con soporte para HTTP/2 y otras mejoras en Windows Server y Windows 10/11).

Buenas prácticas de seguridad en IIS

Aplicar actualizaciones de seguridad de manera oportuna

Configurar actualizaciones automáticas o establecer un ciclo regular de revisión de parches es esencial para proteger el servidor contra las últimas amenazas, incluidas las vulnerabilidades de CVE mencionadas.

Desactivar módulos No utilizados

IIS viene con varios módulos por defecto que podrían aumentar la superficie de ataque. Es recomendable desactivar módulos obsoletos como WebDAV y CGI, que han sido históricamente explotados en ataques de ejecución remota.

Habilitar HTTPS por Defecto

Asegurar que todas las comunicaciones entre los usuarios y el servidor estén encriptadas usando HTTPS. Esto previene ataques de intermediario y protege la transmisión de datos sensibles.

Configurar políticas de seguridad estrictas

Verificar la configuración correcta de los archivos web.config para habilitar cabeceras de seguridad como X-Content-Type-Options, X-Frame-Options y X-XSS-Protection, lo que ayudará a mitigar ataques de inyección y XSS.

Autenticación Fuerte y MFA (Autenticación Multifactor)

Utilizar mecanismos de autenticación seguros, como OAuth o JWT, y habilita la autenticación multifactor (MFA) para las cuentas administrativas del servidor, dificultando los accesos no autorizados.

Monitorización y Auditoría

Implementar herramientas de monitoreo como SIEM para identificar ataques comunes y actividades sospechosas en los logs del servidor IIS. Esto permite una rápida detección y respuesta ante incidentes de seguridad.

Procedimiento para actualizar IIS

1. **Revisar la versión actual de IIS:**
Antes de actualizar, comprueba qué versión está ejecutando el servidor. Esto se puede hacer a través de la consola de administración de IIS o ejecutando el comando: Get-WindowsFeature en PowerShell.

2. **Realizar una copia de seguridad completa del sistema y la configuración de IIS:**Asegurar que todo el sistema, incluida la configuración personalizada de IIS, esté respaldado antes de aplicar cualquier actualización.

3. **Aplicar la actualización más reciente**

Descarga e instala los parches o nuevas versiones desde el centro de actualizaciones de Microsoft o utilizando Windows Update.

4. **Pruebas post-actualización**

Una vez aplicada la actualización, realiza pruebas en todas las aplicaciones web alojadas en IIS para asegurarte de que funcionan correctamente.

COLCERT

Advertencia de Seguridad

Importancia de la Actualización de IIS en sitios Web

COLCERT AD-0810-023

Conclusiones

Mantener actualizado IIS y aplicar configuraciones de seguridad adecuadas es esencial para garantizar un entorno seguro y eficiente. Actualizaciones como IIS 10.0 con soporte para HTTP/2 ofrecen mejoras de rendimiento y seguridad, permitiendo una mejor gestión de recursos y una menor latencia. Es fundamental aprovechar las nuevas funcionalidades y optimizaciones introducidas en las versiones recientes(Microsoft IIS)(Microsoft Learn).

La seguridad en IIS depende no solo de las actualizaciones, sino también de la correcta configuración de los permisos y la desactivación de módulos innecesarios. Minimizar los privilegios de las cuentas de servicio y deshabilitar módulos que no se usen reduce la superficie de ataque y fortalece el entorno de hosting web. Implementar TLS 1.2 o superior para las conexiones cifradas es otra práctica crucial(Microsoft Learn)(Microsoft)).

"Mantener actualizado IIS es crucial para prevenir la explotación de vulnerabilidades críticas, asegurando la protección del servidor frente a posibles ataques que pongan en riesgo la disponibilidad y confidencialidad de los datos sensibles."

Recomendaciones de mitigación para IIS (Internet Information Services) basadas en las mejores prácticas de seguridad y actualizaciones:

- Actualizar siempre a la versión más reciente de IIS 10.0 que viene con Windows Server 2016, 2019 y 2022. Las actualizaciones de seguridad y las mejoras de rendimiento están incluidas en estas versiones.
- Aseura de que el protocolo HTTP/2 esté habilitado en el servidor para mejorar el rendimiento y la seguridad, ya que HTTP/2 reduce la latencia y mejora la eficiencia de la conexión(Microsoft Learn).
- Establecer permisos mínimos para los usuarios que gestionan IIS y sus aplicaciones. Utiliza cuentas específicas de servicio con privilegios reducidos y roles ajustados para limitar el acceso solo a lo necesario.
- Habilitar siempre TLS (Transport Layer Security) y desactiva versiones antiguas como SSL 3.0 y TLS 1.0 que tienen vulnerabilidades conocidas. Usa TLS 1.2 o superior para proteger la transmisión de datos en tu servidor(Microsoft IIS).
- Llevar a cabo auditorías de seguridad y rendimiento regularmente para detectar cualquier anomalía o brecha de seguridad. Esto incluye revisar los logs y realizar pruebas de penetración en las aplicaciones y servicios alojados en IIS.

COLCERT

Advertencia de Seguridad

Importancia de la Actualización de IIS en sitios Web

COLCERT AD-0810-023

Recomendaciones de mitigación para IIS (Internet Information Services) basadas en las mejores prácticas de seguridad y actualizaciones:

- ❑ Revisar los módulos de IIS y deshabilita aquellos que no sean utilizados para reducir la superficie de ataque.

NIVEL DE RIESGO

ALTO

FUENTES:

- Guía de Administración de IIS - https://docs.microsoft.com/es-es/iis/get-started/
- Centro de Seguridad de Microsoft - https://www.microsoft.com/security
- Microsoft Security Response Center (MSRC) - https://msrc.microsoft.com/
- Microsoft Update Catalog - https://www.catalog.update.microsoft.com/Home.aspx
- Boletines de Seguridad de Microsoft - https://docs.microsoft.com/en-us/security-updates/
- •Documentación Oficial de IIS - https://docs.microsoft.com/es-es/iis/
- National Vulnerability Database (NVD) - https://nvd.nist.gov/
- CVE Details - https://www.cvedetails.com/
- Redes Sociales Oficiales de Microsoft Security - https://twitter.com/msftsecurity
- Foros de TechNet de Microsoft - https://social.technet.microsoft.com/forums/en-us/home
- Blog de Seguridad de Microsoft - https://msrc-blog.microsoft.com/