Microsoft anunció planes para reforzar la seguridad de la autenticación de Entra ID al bloquear ataques no autorizados de inyección de scripts dentro de un año.

La actualización de su Política de Seguridad de Contenidos (CSP) busca mejorar la experiencia de inicio de sesión de Entra ID en *"login.microsoftonline[.]com"* al permitir únicamente la ejecución de scripts provenientes de dominios confiables de Microsoft.

"Esta actualización fortalece la seguridad y añade una capa adicional de protección al permitir solo la ejecución de scripts provenientes de dominios confiables de Microsoft durante la autenticación, evitando que código no autorizado o inyectado se ejecute durante el proceso de inicio de sesión," señaló la compañía.

En concreto, solo se permitirá la descarga de scripts desde CDN confiables de Microsoft y la ejecución de scripts internos provenientes de fuentes verificadas por Microsoft. La política renovada se aplicará únicamente a experiencias de inicio de sesión basadas en navegador para direcciones que comiencen con login.microsoftonline.com. Microsoft Entra External ID no se verá afectado.

Este cambio, presentado como una medida preventiva, forma parte de la iniciativa Secure Future Initiative (SFI) de Microsoft y está diseñado para proteger a los usuarios contra ataques de cross-site scripting (XSS), que permiten insertar código malicioso en sitios web. Se espera su implementación global a partir de mediados o finales de octubre de 2026.

Microsoft exhorta a las organizaciones a probar con anticipación sus flujos de inicio de sesión para asegurarse de que no existan inconvenientes ni afectaciones en la experiencia del usuario.

También recomienda evitar el uso de extensiones del navegador o herramientas que inyecten código o scripts en el flujo de autenticación de Microsoft Entra. A quienes dependan de este tipo de herramientas se les sugiere migrar a soluciones que no modifiquen el código del proceso de inicio de sesión.

Para detectar violaciones a CSP, los usuarios pueden ejecutar un flujo de inicio de sesión con la consola de desarrollo abierta y revisar en la herramienta *Console* del navegador si aparecen errores como *"Refused to load the script"*, los cuales indican conflictos con las directivas *"script-src"* o *"nonce"*.

La SFI de Microsoft es un esfuerzo de varios años orientado a priorizar la seguridad en el diseño de nuevos productos y fortalecer la protección ante amenazas cibernéticas cada vez más avanzadas.

Fue presentada inicialmente en noviembre de 2023 y ampliada en mayo de 2024 tras un informe de la Junta de Revisión de Seguridad Cibernética de EE. UU. (CSRB), el cual concluyó que la *"cultura de seguridad de la compañía era insuficiente y necesita una renovación."*

En su tercer informe de progreso, publicado este mes, Microsoft señaló que ha incorporado más de 50 nuevas detecciones en su infraestructura para abordar tácticas, técnicas y procedimientos prioritarios, y que la adopción de autenticación multifactor resistente al phishing (MFA) para usuarios y dispositivos alcanzó el 99.6%.

Otros cambios importantes implementados por Microsoft incluyen:

- Aplicación obligatoria de MFA en todos los servicios, incluso para usuarios de Azure
- Incorporación de capacidades de recuperación automática mediante Quick Machine Recovery, ampliación del soporte para passkeys y Windows Hello, y mejoras en la seguridad de memoria en firmware y controladores UEFI mediante Rust
- Migración del 95% de las máquinas virtuales de firma de Entra ID a Azure Confidential Compute y traslado del 94.3% de la validación de tokens de seguridad a su SDK estándar de identidad
- Eliminación del uso de Active Directory Federation Services (ADFS) en su entorno de productividad
- Retiro de 560,000 inquilinos obsoletos y 83,000 aplicaciones Entra ID sin uso en entornos de producción
- Mejora en la caza de amenazas mediante seguimiento centralizado del 98% de la

infraestructura de producción
- Inventario completo de dispositivos de red y un ciclo de vida de activos más maduro
- Prácticamente todo el código firmado exclusivamente con identidades de producción
- Publicación de 1,096 CVEs, incluidos 53 CVEs de nube sin acción necesaria, y entrega de $17 millones en recompensas

"Para alinearse con los principios de Zero Trust, las organizaciones deben automatizar la detección, respuesta y remediación de vulnerabilidades usando herramientas de seguridad integradas e inteligencia de amenazas," indicó Microsoft. *"Mantener visibilidad en tiempo real de incidentes de seguridad en entornos híbridos y en la nube permite una contención y recuperación más rápidas."*