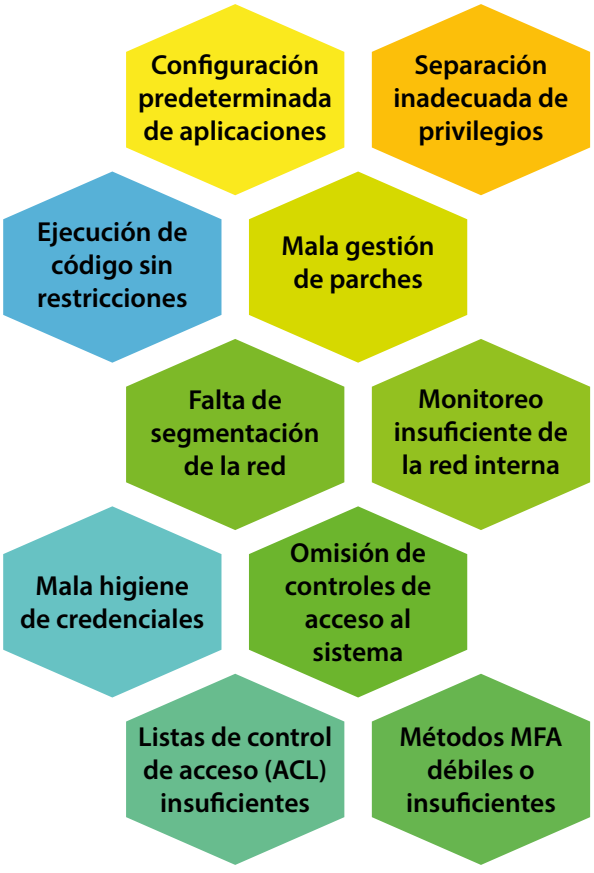
Los diez errores más comunes en ciberseguridad

NSA y CISA destacaron los diez errores de ciberseguridad más importantes en las redes de grandes organizaciones.

Sergiu Gatlan
Bleeping Computer

Fuente en español: *https://blog.segu-info.com.ar/2023/10/top-10-de-errores-de-configuracion-en.html*



Elaboración: *www.segu-info.com.ar*

La Agencia de Seguridad Nacional (NSA) y la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA), de Estados Unidos, revelaron las diez configuraciones erróneas de ciberseguridad más comunes descubiertas por sus equipos rojo y azul en las redes de grandes organizaciones.

Detallan qué tácticas, técnicas y procedimientos (TTP) utilizan los actores de amenazas para explotar con éxito estas configuraciones erróneas con diversos objetivos, incluido obtener acceso, moverse lateralmente y apuntar a información o sistemas confidenciales.

La información incluida en el informe fue recopilada por los Red/Blue Team de las dos agencias durante las evaluaciones y durante las actividades de respuesta a incidentes.

"Estos equipos han evaluado la postura de seguridad de muchas redes en el Departamento de Defensa (DoD), el Poder Ejecutivo Civil Federal (FCEB), los gobiernos estatales, locales, tribales y territoriales (SLTT) y el sector privado", dijo la NSA.

"Estas evaluaciones han demostrado cómo las configuraciones erróneas comunes, como las credenciales predeterminadas, los permisos de servicio y las configuraciones de software y aplicaciones; la separación inadecuada de los privilegios de usuario/administración; la supervisión insuficiente de la red interna; la mala gestión de parches, ponen a todos los estadounidenses en riesgo", dijo Eric Goldstein, subdirector ejecutivo de ciberseguridad de CISA.

Las diez configuraciones de red más frecuentes descubiertas durante las evaluaciones incluyen:

1. Configuraciones predeterminadas de software y aplicaciones.
2. Separación inadecuada de privilegios de usuario/administrador.
3. Monitoreo insuficiente de la red interna.
4. Falta de segmentación de la red.
5. Mala gestión de parches.

6. Omisión de controles de acceso al sistema.
7. Métodos de autenticación multifactor (MFA) débiles o mal configurados.
8. Listas de control de acceso (ACL) insuficientes en recursos compartidos y servicios de red.
9. Mala higiene de credenciales.
10. Ejecución de código sin restricciones.

Esto subraya la necesidad crítica de que los fabricantes de software adopten principios de seguridad desde el diseño

Estas configuraciones erróneas comunes representan vulnerabilidades sistémicas dentro de las redes de numerosas organizaciones grandes. Esto subraya la necesidad crítica de que los fabricantes de software adopten principios de seguridad desde el diseño, mitigando así el riesgo de compromiso.

Goldstein instó a los fabricantes de software a adoptar un conjunto de prácticas proactivas, con el objetivo de abordar eficazmente estas configuraciones erróneas y aliviar los desafíos que enfrentan los defensores de la red.

Estos incluyen la integración de controles de seguridad en la arquitectura del producto desde las etapas iniciales de desarrollo y durante todo el ciclo de vida del desarrollo del software.

Además, los fabricantes deberían dejar de utilizar contraseñas predeterminadas y garantizar que comprometer un único control de seguridad no ponga en peligro la integridad de todo el sistema. También es esencial tomar medidas proactivas para eliminar categorías enteras de vulnerabilidades, como utilizar lenguajes de codificación seguros para la memoria o implementar consultas parametrizadas.

Por último, Goldstein dijo que es imperativo exigir la autenticación multifactor (MFA) para los usuarios privilegiados y establecer MFA como una característica predeterminada, convirtiéndola en una práctica estándar en lugar de una opción opcional.

La NSA y CISA también alientan a los defensores de la red a implementar las medidas de mitigación recomendadas para reducir el riesgo de que los atacantes aprovechen estas configuraciones erróneas comunes.

Las mitigaciones que tendrían este efecto incluyen:

- eliminar las credenciales predeterminadas y fortalecer las configuraciones;
- desactivar servicios no utilizados e implementar estrictos controles de acceso;
- garantizar actualizaciones periódicas y automatizar el proceso de parcheo, dando prioridad al parcheo de vulnerabilidades conocidas que han sido explotadas;
- y reducir, restringir, auditar y monitorear de cerca las cuentas y privilegios administrativos.

Además de aplicar las mitigaciones descritas, las NSA y CISA recomiendan "ejercitar, probar y validar el programa de seguridad de su organización contra los comportamientos de amenazas asignados al marco MITRE ATT&CK for Enterprise". Las dos agencias federales también recomiendan probar el inventario de controles de seguridad existentes para evaluar su desempeño frente a las técnicas de ATT&CK descritas en el aviso.

La NSA y CISA también alientan a los defensores de la red a implementar las medidas de mitigación recomendadas para reducir el riesgo