[Publish] - 14. Habilitar IMDSv2 en EC2

El hallazgo de seguridad **"Habilitar IMDSv2 en EC2"** se refiere a la necesidad de utilizar la versión más segura del **Servicio de Metadatos de Instancia (IMDS)**. Este servicio es un componente crucial en EC2 que permite a las aplicaciones que corren dentro de una instancia obtener metadatos y credenciales de seguridad temporales sin necesidad de almacenarlas en el código.

Existen dos versiones:

- **IMDSv1 (Heredada):** Es un modelo de solicitud/respuesta simple. Es vulnerable a ciertos tipos de ataques, principalmente **SSRF (Server-Side Request Forgery)**. Un atacante que explote una vulnerabilidad SSRF en una aplicación web podría engañar al servidor para que solicite las credenciales del IMDS y las filtre.
- **IMDSv2 (Seguro):** Introduce un método de solicitud orientado a sesiones. Antes de poder solicitar los metadatos, la aplicación debe crear una sesión con un token de un solo uso. Este simple paso mitiga eficazmente los ataques SSRF, ya que un atacante no puede crear esa sesión desde el exterior.

Forzar el uso de IMDSv2 es una medida de seguridad fundamental para proteger las credenciales temporales de tus instancias y prevenir que un atacante pueda moverse lateralmente en tu entorno de AWS.

Análisis de las Instancias Reportadas

Las siguientes instancias de EC2 han sido identificadas por no requerir el uso de IMDSv2, lo que las deja potencialmente vulnerables.

Type	Name	Account Number
Instance	i-000fbf2a79f92c3ab	002670977573
Instance	i-0097dc2f5bc287109	002670977573
Instance	i-00d18f0f2489d5748	890342916428
Instance	i-0102bd635a284e84e	398984081329
Instance	i-0118cb2e1c48089ff	002670977573
Instance	i-0118ff93c3766f93b	002670977573
Instance	i-0135d3e4d74609572	002670977573

Instance	i-017853c6643601641	002670977573
Instance	i-0195867f8c0aa2c79	002670977573
Instance	i-01bcd4c331a68a6a2	002670977573
Instance	i-0201d025e251cce12	002670977573
Instance	i-02107fa019533cfc9	002670977573
Instance	i-025714965e3a949f0	002670977573
Instance	i-0361d9073c0b9d8da	002670977573
Instance	i-0370e6a66e2bb202e	398984081329
Instance	i-0375aeb0c2e4d3607	002670977573
Instance	i-0375b08b8377e65f4	002670977573
Instance	i-03c171fa80e8824ff	002670977573
Instance	i-03c8a35067b84638d	398984081329
Instance	i-03d3268361158a5cc	002670977573
Instance	i-03ea3bdeea26ae150	398984081329
Instance	i-044ed9556b72bf573	002670977573
Instance	i-046ceefd81c10686e	890342916428
Instance	i-04aa2e5982c74273f	890342916428
Instance	i-04ce7e0f7ee914dad	002670977573
Instance	i-054f00812fab2a4f9	002670977573
Instance	i-05545802b22afd142	002670977573
Instance	i-0559c8024ad0faf0b	890342916428
Instance	i-057082e3663b766a9	890342916428
Instance	i-05786c8888262fa7a	002670977573
Instance	i-05fbfb9d8a620ecc7	613703092215
Instance	i-060952b97ecbb5ea3	890342916428

Instance	i-06131485aa51c1563	613703092215
Instance	i-06915e3e672b0a8cf	002670977573
Instance	i-06ad74674e8a48f89	002670977573
Instance	i-06af34899b8ab0913	002670977573
Instance	i-06fe4642fc9338d60	398984081329
Instance	i-07554df176f70b0d2	002670977573
Instance	i-0773a446fabab9981	890342916428
Instance	i-079e7eb2666f902c6	002670977573
Instance	i-083b8a90b48de6e49	398984081329
Instance	i-085224b6e33b24fad	002670977573
Instance	i-0855a67c9803befd4	002670977573
Instance	i-087fb602b20252e59	890342916428
Instance	i-08b195de7ac76cf0b	002670977573
Instance	i-08e561cb0648b48e7	002670977573
Instance	i-08e60134966ec5a6b	002670977573
Instance	i-08f0c6ec87a595923	002670977573
Instance	i-0903fa6b6abec761e	002670977573
Instance	i-092ac23d761c67be1	002670977573
Instance	i-095bb40653ef2d7e0	890342916428
Instance	i-09c8ea427f61934c0	002670977573
Instance	i-09d82919d2e96e71b	002670977573
Instance	i-09e67761338c6c937	002670977573
Instance	i-0a3dc851efc9b9949	890342916428
Instance	i-0a4d4b0cac465d090	398984081329
Instance	i-0a59a83c85bb62e27	890342916428

Instance	i-0a70ed56f594c86c6	890342916428
Instance	i-0a7aaf6a2b4078899	002670977573
Instance	i-0ab7c03cebd52828e	002670977573
Instance	i-0acf4b80216e0bbf8	002670977573
Instance	i-0aea114ebcc9fe154	613703092215
Instance	i-0af65d815395fb91a	002670977573
Instance	i-0be60800aa1e9d9a5	613703092215
Instance	i-0c0189f0c6f1e66db	398984081329
Instance	i-0c053af98d825f427	613703092215
Instance	i-0c44bb9dfa5f0cff5	002670977573
Instance	i-0c4730320e45e503d	002670977573
Instance	i-0c93846849a4a1ed6	890342916428
Instance	i-0c9842f8d11cf184a	002670977573
Instance	i-0c9c0b6ef36d57332	002670977573
Instance	i-0cdd21e9bd5de13e1	002670977573
Instance	i-0ce94d3dabf70e6f7	890342916428
Instance	i-0cf943ec1228fe4b8	002670977573
Instance	i-0d2eb8da875d4814b	398984081329
Instance	i-0d3a5cc895c2290c6	613703092215
Instance	i-0d99b7287573033fd	002670977573
Instance	i-0ddb2c8b93ac9d4f9	002670977573
Instance	i-0df3ee6bae187f599	398984081329
Instance	i-0e28cafe31926d286	002670977573
Instance	i-0e31a36f1fd1a0b9d	398984081329
Instance	i-0e3d8c08fe0f3e007	002670977573

Instance	i-0e564a829eefbb96c	398984081329
Instance	i-0e89d27346605358f	890342916428
Instance	i-0eca0290b4de12fb5	002670977573
Instance	i-0f1df26d17b3a3ac0	890342916428
Instance	i-0fce67638c6fa20fb	890342916428

Preguntas para tu Equipo (Acción Requerida)

La transición a IMDSv2 debe ser validada para asegurar que no interrumpa las aplicaciones.

1. **Compatibilidad de Software:** ¿Pueden confirmar que el software y los SDKs de AWS que se ejecutan en estas instancias son compatibles con IMDSv2? La mayoría de los SDKs de AWS actualizados a partir de finales de 2019 son compatibles. Las aplicaciones más antiguas o personalizadas que acceden directamente a la URL de metadatos podrían necesitar una actualización.
2. **Plan de Pruebas:** ¿Se recomienda realizar el cambio primero en una instancia de un entorno de no producción (desarrollo o QA) para validar que las aplicaciones siguen funcionando correctamente antes de aplicar el cambio en producción?

Consideraciones de Costo

No hay **ningún costo directo** asociado con el uso o la exigencia de IMDSv2. Es una mejora de seguridad fundamental proporcionada por AWS sin cargo adicional.

Cómo Solucionarlo: Forzar el Uso de IMDSv2

Puedes modificar una instancia en ejecución para que requiera IMDSv2.

1. **Navegar a la Instancia en la Consola:**
   - Ve a la consola de **EC2**.
   - Selecciona una de las instancias de la lista.
2. **Modificar las Opciones de la Instancia:**
   - Haz clic en el menú **Acciones**, luego en **Configuración de la instancia** y finalmente en **Modificar opciones de metadatos de la instancia**.
3. **Configurar IMDSv2:**
   - En la ventana de diálogo, asegúrate de que **Servicio de metadatos de instancia** esté **Habilitado**.
   - Para la opción **Versión de metadatos**, selecciona **V2 (token requerido)**. Esto forzará a que todas las solicitudes al servicio de metadatos usen el método de sesión de IMDSv2.

- Haz clic en **Guardar**.

4. **Repetir y Validar:**
   - Repite este proceso para todas las instancias listadas, preferiblemente comenzando con entornos de no producción.
   - Después de aplicar el cambio, valida que las aplicaciones en la instancia sigan funcionando como se espera y puedan obtener sus credenciales de IAM correctamente.

Recomendación

Se recomienda que se configure la exigencia de **IMDSv2 (token requerido)** en todas las instancias de EC2 listadas. Comiencen con los entornos de desarrollo y prueba para validar la compatibilidad y luego procedan con los entornos de producción.

Además, es una buena práctica configurar todas las nuevas plantillas de lanzamiento (Launch Templates) y AMIs para que requieran IMDSv2 por defecto, asegurando así que todas las futuras instancias se desplieguen con esta configuración de seguridad mejorada desde el principio.

Referencias

Use the Instance Metadata Service to access instance metadata - Amazon Elastic Compute Cloud