La empresa de ciberseguridad en la nube Wiz reveló que detectó explotación activa de una vulnerabilidad en una herramienta de Linux llamada Pandoc, utilizada en ataques con el objetivo de infiltrarse en el servicio Instance Metadata Service (IMDS) de Amazon Web Services (AWS).

La falla, identificada como CVE-2025-51591 (puntaje CVSS: 6.5), corresponde a un caso de Server-Side Request Forgery (SSRF), que permite a un atacante comprometer un sistema mediante la inyección de un elemento HTML *iframe* especialmente manipulado.

El servicio IMDS de EC2 es un componente esencial del entorno de AWS, ya que proporciona información de las instancias en ejecución y credenciales temporales en caso de que la instancia tenga un rol de identidad y acceso (IAM) asignado. Esta metadata puede ser consultada desde cualquier aplicación en la instancia EC2 a través de la dirección local 169.254.169[.]254.

Dichas credenciales permiten interactuar de forma segura con otros servicios de AWS como S3, RDS o DynamoDB, evitando almacenar llaves directamente en la máquina y reduciendo así el riesgo de exposición accidental.

Una técnica frecuente para robar credenciales de IAM en IMDS es explotar vulnerabilidades SSRF en aplicaciones web. Básicamente, se engaña a la aplicación en ejecución para que envíe peticiones al servicio IMDS en busca de credenciales.

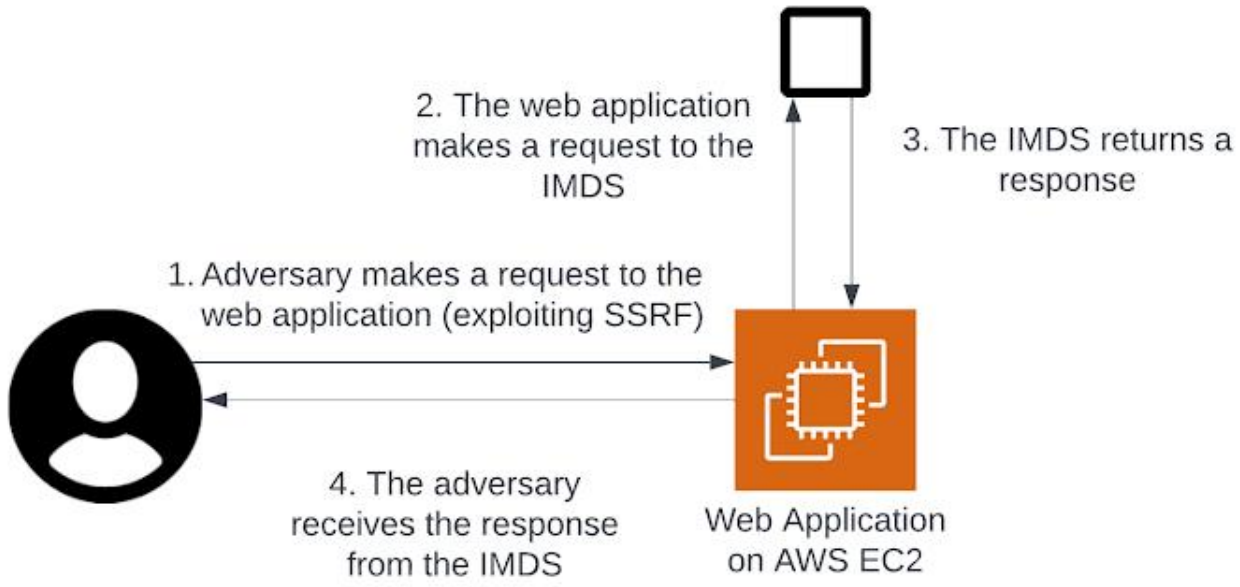
"Si la aplicación puede alcanzar el endpoint de IMDS y es vulnerable a SSRF, el atacante puede obtener credenciales temporales sin necesidad de acceso directo al host (como RCE o traversal de rutas)," explicaron las investigadoras de Wiz, Hila Ramati y Gili Tikochinski.

Esto implica que un adversario interesado en la infraestructura de AWS puede buscar fallas de SSRF en aplicaciones web alojadas en EC2 y, al encontrarlas, acceder a la metadata de la instancia para sustraer credenciales IAM. No se trata de un riesgo hipotético.

En 2022, la firma Mandiant (propiedad de Google) descubrió que un grupo de amenazas,

identificado como UNC2903, abusó de credenciales obtenidas vía IMDS desde julio de 2021. Para ello explotaron una vulnerabilidad SSRF (CVE-2021-21311, puntaje CVSS: 7.2) en Adminer, una herramienta de gestión de bases de datos de código abierto, con el fin de robar información.

El problema radica en que IMDSv1 funciona bajo un esquema de petición y respuesta, lo que lo hace atractivo para atacantes que buscan aplicaciones web vulnerables que lo utilicen.



En un informe reciente, Resecurity advirtió que la explotación de SSRF en entornos de nube como AWS puede tener *"consecuencias graves y de gran alcance,"* incluyendo robo de credenciales, reconocimiento de red y acceso no autorizado a servicios internos.

"Como el SSRF se origina dentro del servidor, puede llegar a endpoints protegidos por firewalls perimetrales. En la práctica convierte a la aplicación vulnerable en un proxy, permitiendo al atacante saltar listas blancas de IP y alcanzar activos internos que de otro

modo serían inaccesibles," señaló la firma.

Los hallazgos más recientes de Wiz confirman que los ataques contra IMDS siguen activos, ahora explotando vulnerabilidades SSRF en aplicaciones poco conocidas como Pandoc.

"La vulnerabilidad, registrada como CVE-2025-51591, surge de la forma en que Pandoc procesa etiquetas en documentos HTML," dijeron los investigadores. *"Esto permite a un atacante crear un que apunte al servidor IMDS u otros recursos privados."*

"El atacante envió documentos HTML manipulados con elementos cuyo atributo src estaba dirigido al endpoint IMDS de AWS (169.254.169[.]254). El objetivo era renderizar y extraer información sensible de rutas como /latest/meta-data/iam/info y /latest/meta-data/iam," añadieron.

El ataque finalmente no tuvo éxito debido a que estaba habilitado IMDSv2, que requiere primero obtener un token y usarlo en todas las solicitudes mediante un encabezado especial (*X-aws-ec2-metadata-token*), lo que mitiga los intentos de SSRF.

La compañía informó a *The Hacker News* que observó intentos de explotación *"desde agosto y durante varias semanas,"* y que también identificó esfuerzos de actores desconocidos para aprovechar otra vulnerabilidad SSRF en ClickHouse con el fin de atacar sin éxito la nube de Google.

Para reducir el riesgo de CVE-2025-51591 en entornos de nube, se recomienda usar la opción *-f html+raw_html* o *–sandbox* para evitar que Pandoc procese contenido de iframes a través del atributo *src*.

"[Los responsables de Pandoc] decidieron que renderizar iframes es el comportamiento esperado y que el usuario debe encargarse de sanitizar la entrada o usar las banderas de sandbox cuando maneja inputs externos," explicó Wiz.

Por su parte, Mandiant advirtió: *"Aunque Amazon recomienda usar IMDSv2 con las mejoras*

de GuardDuty, las instancias EC2 creadas por clientes que aún empleen IMDSv1 pueden estar en riesgo si además ejecutan software de terceros vulnerable y sin parchear.”

La recomendación general es aplicar IMDSv2 en todas las instancias EC2 y asegurarse de que los roles asignados sigan el principio de privilegio mínimo (PoLP) para limitar el alcance de un posible compromiso.