La Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA) ha incorporado dos fallos de seguridad que afectan a Adobe ColdFusion y Oracle Agile Product Lifecycle Management (PLM) a su lista de Vulnerabilidades Explotadas Conocidas (KEV), basándose en evidencia de ataques en curso.

Las vulnerabilidades identificadas son las siguientes:

- CVE-2017-3066 (Puntuación CVSS: 9.8): Un problema de deserialización en Adobe ColdFusion dentro de la biblioteca Apache BlazeDS que permite la ejecución de código arbitrario. (Solucionado en abril de 2017).
- CVE-2024-20953 (Puntuación CVSS: 8.8): Una vulnerabilidad de deserialización en Oracle Agile PLM que posibilita que un atacante con bajos privilegios y acceso a la red a través de HTTP comprometa el sistema. (Corregida en enero de 2024).

Aún no se han publicado informes públicos que confirmen la explotación de estas vulnerabilidades. No obstante, otra falla que también afecta a Oracle Agile PLM (CVE-2024-21287, con una puntuación CVSS de 7.5) fue objeto de ataques a finales del año pasado.

Para reducir los riesgos de posibles ataques que aprovechen estas debilidades, se recomienda a los usuarios instalar las actualizaciones correspondientes. Las agencias federales tienen como fecha límite el 17 de marzo de 2025 para reforzar la seguridad de sus redes frente a estas amenazas.

Este anuncio coincide con el descubrimiento de la firma de ciberseguridad GreyNoise, que ha detectado intentos activos de explotación de CVE-2023-20198, una vulnerabilidad previamente corregida en dispositivos Cisco.

Se han identificado 110 direcciones IP maliciosas, con la mayoría de ellas provenientes de Bulgaria, Brasil y Singapur, relacionadas con estos ataques.

> *«En diciembre de 2024 y enero de 2025, dos direcciones IP maliciosas explotaron CVE-2018-0171, con origen en Suiza y Estados Unidos. Este período coincide con las acciones de Salt Typhoon, un grupo de amenazas vinculado al gobierno chino, que presuntamente comprometió redes de telecomunicaciones utilizando CVE-2023-20198 y CVE-2023-20273«,* informó el equipo de investigación de GreyNoise.