La Agencia de Seguridad de Infraestructura y Ciberseguridad de los Estados Unidos (CISA) incluyó recientemente una vulnerabilidad de alta criticidad, ya corregida, que afecta al software USAHERDS de Acclaim Systems, en su catálogo de Vulnerabilidades Explotadas Conocidas (KEV). Esta decisión se basa en pruebas de que dicha vulnerabilidad está siendo explotada activamente en entornos reales.

La vulnerabilidad, identificada como CVE-2021-44207 (puntuación CVSS: 8.1), se debe al uso de credenciales estáticas y codificadas en USAHERDS, lo que podría permitir a un atacante ejecutar código arbitrario en servidores vulnerables.

El problema está relacionado con la utilización de valores predeterminados para las claves `ValidationKey` y `DecryptionKey` en la versión 7.4.0.1 y anteriores. Estos valores podrían ser aprovechados por un atacante para obtener acceso remoto al servidor que ejecuta la aplicación. Sin embargo, el atacante primero tendría que acceder a estas claves mediante otros métodos.

> *«Estas claves se utilizan para proteger el ViewState de la aplicación. Un atacante con conocimiento de estas claves podría manipular el servidor para deserializar datos de ViewState creados maliciosamente»*, explicó Mandiant, una empresa de Google, en un informe publicado en diciembre de 2021.
>
> *«Un ciberdelincuente que tenga acceso a las claves `validationKey` y `decryptionKey` de una aplicación web puede generar un ViewState malicioso que supere la verificación MAC y que el servidor deserialice. Este proceso podría llevar a la ejecución de código en el servidor.»*

Aunque no se han reportado incidentes recientes que exploten la CVE-2021-44207, se sabe que el grupo de amenazas APT41, vinculado a China, utilizó esta vulnerabilidad como un día cero en 2021, durante ataques dirigidos a las redes gubernamentales de seis estados en Estados Unidos.

A las agencias del Ramo Ejecutivo Civil Federal (FCEB) se les recomienda implementar las soluciones proporcionadas por el fabricante antes del 13 de enero de 2025 para proteger sus sistemas frente a posibles amenazas.

Por otro lado, Adobe ha informado sobre una falla crítica de seguridad en ColdFusion, identificada como CVE-2024-53961 (puntuación CVSS: 7.8). Esta vulnerabilidad ya cuenta con una prueba de concepto (PoC) que podría ser utilizada para leer arbitrariamente el sistema de archivos.

Adobe ha corregido este problema en las versiones ColdFusion 2021 Update 18 y ColdFusion 2023 Update 12. Se insta a los usuarios a aplicar estos parches de manera inmediata para evitar posibles riesgos de seguridad.