Hewlett Packard Enterprise (HPE) corrigió una vulnerabilidad de gravedad máxima en el software OneView que, de ser explotada con éxito, podría permitir la ejecución remota de código.

La falla crítica, identificada como CVE-2025-37164, cuenta con una puntuación CVSS de 10.0. HPE OneView es una plataforma de gestión de infraestructura de TI diseñada para simplificar las operaciones y administrar todos los sistemas desde un panel centralizado.

"Se ha identificado una posible vulnerabilidad de seguridad en el software Hewlett Packard Enterprise OneView. Esta vulnerabilidad podría ser explotada, permitiendo que un usuario remoto no autenticado lleve a cabo la ejecución remota de código", señaló HPE en un aviso de seguridad publicado esta semana.

El problema afecta a todas las versiones anteriores a la 11.00, versión que ya incluye la corrección. Además, la empresa puso a disposición un hotfix aplicable a las versiones de OneView 5.20 a 10.20.

Cabe destacar que este hotfix debe reinstalarse tras actualizar desde la versión 6.60 o posterior a la 7.00.00, así como después de cualquier proceso de reimagen del HPE Synergy Composer. Existen parches independientes tanto para la appliance virtual de OneView como para Synergy Composer2.

Aunque HPE no ha informado que la vulnerabilidad esté siendo explotada activamente, es fundamental que los usuarios instalen las actualizaciones lo antes posible para garantizar una protección adecuada.

A principios de junio, la compañía también publicó correcciones para ocho vulnerabilidades en su solución de respaldo y deduplicación de datos StoreOnce, las cuales podían derivar en elusión de autenticación y ejecución remota de código. Asimismo, lanzó OneView versión 10.00 para solucionar múltiples fallas conocidas en componentes de terceros, incluidos Apache Tomcat y Apache HTTP Server.