Apache lanza parche para exploits de día cero activos en la naturaleza

Autor: I. Stepanenko

Fecha: Sunday 24th of October 2021 05:22:15 AM

Apache emitió parches para abordar dos vulnerabilidades de seguridad, incluyendo un cruce de ruta y una falla de divulgación de archivos en su servidor HTTP que, según dijo, está siendo explotado activamente en la naturaleza.

> «Se encontró una falla en un cambio realizado en la normalización de rutas en Apache HTTP Server 2.4.49. Un atacante podría usar un ataque de ruta transversal para mapear URLs a archivos fuera de la raíz esperada del documento», dijeron los responsables del proyecto de código abierto.

> «Si los archivos fuera de la raíz del documento no están protegidos por 'requerir todos denegados', estas solicitudes pueden tener éxito. Además, esta falla podría filtrar la fuente de archivos interpretados como scripts CGI».

La vulnerabilidad, rastreada como CVE-2021-41773, afecta solo al servidor Apache HTTP versión 2.4.49. Se le atribuye el crédito por informar el problema el 29 de septiembre a Ash Daulton y al equipo de seguridad de cPanel.

Apache también resolvió una vulnerabilidad de desreferencia de puntero nulo observada durante el procesamiento de solicitudes HTTP/2 (CVE-2021-41524), lo que permite que un adversario realice un ataque de denegación de servicio (DoS) en el servidor. La corporación sin fines de lucro dijo que la vulnerabilidad se introdujo en la versión 2.4.49.

Se recomienda a los usuarios de Apache que parcheen lo antes posible para contener la vulnerabilidad de recorrido de ruta y mitigar cualquier riesgo asociado con la explotación activa de la falla.