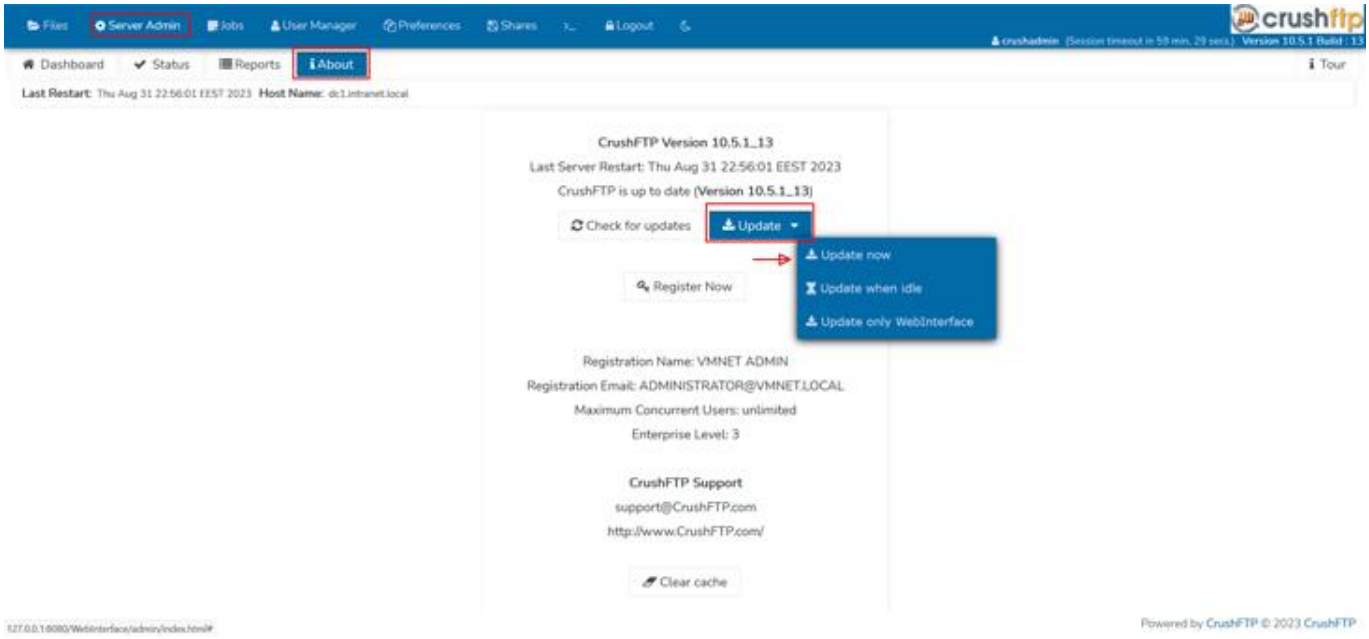
Los usuarios del software de transferencia de archivos empresarial CrushFTP están siendo instados a actualizar a la versión más reciente después de que se descubriera una vulnerabilidad de seguridad que está siendo aprovechada de manera dirigida en la naturaleza.

> *«Las versiones de CrushFTP v11 anteriores a la 11.1 presentan una vulnerabilidad que permite a los usuarios escapar de su VFS y descargar archivos del sistema. Esta vulnerabilidad ha sido corregida en la versión v11.1.0»*, indicó CrushFTP en un aviso emitido el viernes.

Sin embargo, los clientes que operan sus instancias de CrushFTP dentro de un entorno restringido de DMZ (zona desmilitarizada) están protegidos contra estos ataques.

Simon Garrelou del equipo de seguridad informática de Airbus (CERT) ha sido reconocido por descubrir y reportar esta falla. Todavía no se le ha asignado un identificador CVE.

La empresa de ciberseguridad CrowdStrike, en una publicación compartida en Reddit, informó que han detectado un exploit para esta vulnerabilidad siendo utilizado en la naturaleza de manera «selectiva».



Se dice que estas intrusiones han apuntado principalmente a entidades estadounidenses, con la actividad de recopilación de inteligencia sospechada de tener motivaciones políticas.

> *«Los usuarios de CrushFTP deben seguir consultando el sitio web del proveedor para obtener las instrucciones más actualizadas y dar prioridad a la aplicación de parches»,* recomendó CrowdStrike.