Una falla crítica de seguridad recientemente revelada en CrushFTP está siendo activamente explotada en entornos reales. Identificada como CVE-2025-54309, esta vulnerabilidad tiene una puntuación CVSS de 9.0.

"CrushFTP 10 antes de la versión 10.8.5 y 11 antes de la 11.3.4_23, cuando no se utiliza la funcionalidad de proxy DMZ, maneja incorrectamente la validación AS2, lo que permite a atacantes remotos obtener acceso administrativo a través de HTTPS", según la descripción publicada en la Base de Datos Nacional de Vulnerabilidades (NVD) del NIST.

En un boletín de seguridad, CrushFTP informó que detectó por primera vez la explotación activa de esta vulnerabilidad de día cero el 18 de julio de 2025 a las 9 a.m. CST, aunque reconoció que el fallo podría haber sido aprovechado desde antes.

"El vector de ataque fue HTTP(S), que utilizaron para vulnerar el servidor", explicó la empresa. *"Habíamos corregido otro problema relacionado con AS2 en HTTP(S), sin darnos cuenta de que un fallo anterior podía ser explotado de esta forma. Al parecer, los atacantes notaron el cambio en nuestro código y descubrieron cómo aprovechar la vulnerabilidad previa"*.

CrushFTP se utiliza ampliamente en sectores gubernamentales, sanitarios y corporativos para gestionar transferencias de archivos sensibles, lo que hace que el acceso administrativo comprometido sea especialmente grave. Una instancia vulnerada puede permitir la exfiltración de datos, la instalación de puertas traseras o el movimiento lateral hacia sistemas internos que dependen del servidor para intercambios seguros. Sin el aislamiento de una DMZ, la instancia queda expuesta como un punto único de falla.

La compañía señaló que los actores maliciosos responsables lograron realizar ingeniería inversa sobre el código fuente y detectaron el fallo para atacar dispositivos que aún no han sido actualizados. Se cree que la vulnerabilidad CVE-2025-54309 estaba presente en compilaciones de CrushFTP anteriores al 1 de julio.

CrushFTP también publicó los siguientes indicadores de compromiso (IoCs):

- El usuario predeterminado tiene privilegios de administrador
- Creación de identificadores de usuario aleatorios largos (por ejemplo: `7a0d26089ac528941bf8cb998d97f408m`)
- Nuevos nombres de usuario creados con acceso administrativo
- El archivo *«MainUsers/default/user.xml»* fue modificado recientemente y contiene un valor en *«last_logins»*
- Elementos de la interfaz web para usuarios desaparecieron, y algunos usuarios normales ahora presentan un botón de administración

Los equipos de seguridad que investiguen posibles compromisos deben revisar los tiempos de modificación del archivo *user.xml*, correlacionar los eventos de inicio de sesión de administradores con direcciones IP públicas y auditar los cambios de permisos en carpetas críticas. También es vital buscar patrones anómalos en los registros de acceso asociados a nuevos usuarios o elevaciones de privilegios no justificadas, indicios comunes de explotación posterior a una intrusión.

Como medidas de mitigación, la empresa recomienda restaurar la configuración del usuario predeterminado desde las copias de seguridad, así como revisar los reportes de carga/descarga para detectar transferencias sospechosas. Otras recomendaciones incluyen:

- Limitar las direcciones IP autorizadas para acciones administrativas
- Establecer listas blancas de IPs que puedan conectarse al servidor CrushFTP
- Usar una instancia de CrushFTP en DMZ para entornos empresariales
- Verificar que las actualizaciones automáticas estén habilitadas

Por ahora, se desconoce el alcance exacto de los ataques que explotan esta falla. En abril pasado, otra vulnerabilidad en la misma solución (CVE-2025-31161, puntuación CVSS: 9.8) fue utilizada para distribuir el agente MeshCentral y otros tipos de malware.

El año anterior, también se descubrió que una segunda vulnerabilidad crítica en CrushFTP (CVE-2024-4040, CVSS: 9.8) fue explotada por actores maliciosos para atacar a múltiples entidades en EE.UU.

Dada la explotación repetida de vulnerabilidades de alta gravedad en el último año, CrushFTP se ha convertido en un objetivo frecuente de campañas de amenazas avanzadas. Las organizaciones deben considerar este patrón dentro de sus evaluaciones de exposición al riesgo, junto con la gestión de parches, amenazas asociadas a soluciones de transferencia de archivos de terceros y procesos de detección de días cero vinculados a accesos remotos y robo de credenciales.