OpenSSH, la utilidad más popular de Internet para la administración de servidores remotos, agregó soporte para el protocolo FIDO/U2F.

De este modo, a partir de OpenSSH 8.2, los usuarios pueden configurar una clave de seguridad de hardware al autenticarse por medio de SSH en un servidor remoto.

Después de que los usuarios inicien sesión en un servidor utilizando su nombre de usuario y contraseña, o un certificado de autenticación SSH, deberán presentar una clave de seguridad basada en FIDO/U2F USB, Bluetooth o NFC como segunda prueba de identidad.

El uso de una clave de seguridad se considera actualmente uno de los métodos de autenticación multifactor (MFA) más potentes que se conocen en la actualidad.

El uso de MFA, comúnmente conocido como 2FA, es la forma más sencilla de evitar que los hackers adivinen o realicen ataques de fuerza bruta contra contraseñas SSH y obtengan el control de los servidores.

El año pasado, Microsoft dijo que los clientes de la compañía que habilitaron MFA para sus respectivas cuentas de Microsoft, bloquearon el 99.9% de los intentos de pirateo de cuentas, lo que muestra lo difícil que es eludir una solución MFA en la actualidad.

En una tabla que Microsoft publicó en octubre, calificó las claves de seguridad de hardware basadas en FIDO como la solución MFA más segura y más difícil de descifrar.

Las instrucciones para configurar las primeras claves de seguridad de hardware con OpenSSH se incluyen en las notas de revisión de la versión 8.2.