

26 March 2008

By: Bogdan Botezatu, Hardware Editor



The Corsair Flash Padlock: Before Corsair

[Hacking Into Others' Data Made Simple: the Corsair Padlock Workaround](#)

Corsair's Padlock USB stick is accessible to anyone who has basic soldering skills

The promised data security for mobile storage device is slowly but surely being dismantled piece by piece. You may remember our previous reports about [defeated biometric security](#) using open-source software; however, this new episode of "Poking into other's data" series takes hacking into the hardware playground. Corsair's Flash Padlock pen drive was touted as being one of the most secure external storage media. The unit comes with built-in hardware DataLock encryption, delivered by a less known manufacturer, called ClevX. The pen drive has the same basic working principle as an ATM, where users have to enter a personal 1 to 10 digit code to get access to the stored data. The protection scheme surely seems interesting, but, according to the Dutch tech site [TweakBlogs](#), it can be easily defeated at the cost of just a few cents. The workaround does not involve additional software; however, in order to get to the encrypted data, you must have physical access to the drive and some basic soldering skills. The hacking process begins with cracking the flash drive open. This is the most important step in this not-so-legit activity, and the wannabe hacker should pay extra attention while "peeling off" the drive's shell, in order not to damage the fragile components underneath. Once the drive's internals are exposed, the actual hacking is nothing more than soldering a small, 10 Kilo-ohm resistor in such a way to create a resistive bridge between the USB port's ground and the ML connector on the top-right side of the flash pen, which concludes the hacking part. When plugged into the USB port, the drive gets unlocked by default, and the allegedly protected data can be accessed immediately. When talking about mobile storage devices, data security is a critical aspect, as they can easily get misplaced, lost or even stolen. That is why users should not rely on the protection methods delivered out-of-the-box. Adding an extra layer of data encryption on top of the disk's built-in security won't prevent motivated hackers from poking into your data, but it would surely give them a hard time.