nexthardware.com

a cura di: **Giuseppe Apollo - pippo369 - 15-06-2012 12:00**

Non risolvibile via firmware il problema della crittografia AES 256-bit per i SandForce SF-2281

LINK (https://www.nexthardware.com/news/ssd-hard-disk-masterizzatori/4729/non-risolvibile-via-firmware-il-problema-della-crittografia-aes-256-bit-per-i-sandforce-sf-2281.htm)

Più grave del previsto il bug dei SandForce SF-2281 di cui si è tanto discusso in questi giorni.

↔

LSI ha confermato in un comunicato stampa che il controller↔ SandForce SF-2281 non offre il corretto supporto per la crittografia AES-256 come in precedenza era stato affermato.

Diversamente dalle prime ottimistiche voci circolate in rete, il problema del circuito che gestisce la crittografia AES 256-bit non è risolvibile con una patch software, ma soltanto con una correzione hardware.

LSI vende i controller SandForce alla stragrande maggioranza di produttori di↔ SSD e, molti di questi, tra cui Intel, hanno fatto annunci ufficiali riguardo a questo problema.

Intel al riguardo, ha annunciato che i clienti per il quale la mancanza della crittografia AES 256-bit possa costituire un serio problema, possono restituire i loro SSD Intel 520 entro il 1 ottobre 2012 ed ottenere indietro il denaro investito.

Intel sottolinea inoltre che lavorerà per il lancio di nuove unità SSD con l'AES 256-bit funzionante ed LSI conferma che sta cercando di risolvere il problema del SandForce SF-2281 nel più breve tempo possibile.

Kingston, che utilizza il controller SandForce SF-2281 in parecchie linee di prodotti, ha annunciato che i clienti possessori di SSD della serie↔ SSDNow V 200 e KC100 possono contattare il servizio clienti per↔ sostituire le proprie unità SSD con i modelli aggiornati e che i suoi tecnici stanno lavorando a stretto contatto con quelli↔ LSI per risolvere il problema.

Per gli utenti normali che non utilizzano la crittografia AES o possono accontentarsi di una doppia crittografia↔ AES a 128 bit, l'SF-2281 funziona correttamente, quindi il produttore non effettuerà sostituzioni su quei prodotti che pur montando il controller incriminato non sono certificati per funzionare

con AES 256-bit.

↔

↔