Flaws in major encrypting SSDs allow attackers to bypass encryption and decrypt data

Submitted by: iStorage Limited
Thursday, 8 November 2018

(London, Nov 2018), Researchers at Radbound University in the Netherlands revealed that major flaws in some Solid State Drives (SSDs) allow an attacker to bypass the password-based authentication process and access encrypted data stored on the drives.

The researchers found that the data encryption keys used to secure data stored on the drives are not derived from the owner’s password, and that an attacker with physical access to the drives can reprogram the drives via a debug port in order to accept any password. Once the drives have been reprogrammed, the SSDs will use the stored Data Encryption Keys to encrypt and decrypt all stored data.

With questions now arising into just how safe hardware encrypted SSDs are, John Michael, CEO, iStorage Limited stated:

“This is an extremely worrying issue for anyone who has purchased such Self Encrypting SSDs believing that their data is encrypted and secure. According to researchers at Radbound University, the flaws range from very easy to slightly more complicated. ZDnet (https://www.zdnet.com/article/flaws-in-self-encrypting-ssds-let-attackers-bypass-disk-encryption/) reported that they found that certain Self Encrypting SSDs come with support for a “master password”, which is written in the manual and can be used to gain access to the user’s encrypted password, effectively bypassing the user’s custom password. The other vulnerability relates to the user-chosen password not being linked to the Data Encryption Key, allowing an attacker to reprogram the drives’ debug port in order to accept any password and access all data contained therein.

{{Our customers need not be concerned about these flaws being present in iStorage products. iStorage products are not vulnerable to any such attacks reported by the researchers. The iStorage generated Data Encryption Key, in very simple terms, is derived from the PIN that is configured and entered by the user on the onboard keypad. In addition, they incorporate a lock-down feature which prevents any attacker from reprogramming our firmware. Furthermore, the iStorage Common Criteria EAL4+ ready microprocessor, employs a flash lock mechanism that ensures the product constantly remains in a mode where all write-access to program memory is denied.

Unlike other similar so-called password-based and PIN authenticated products, iStorage products such as the diskAshur², diskAshur PRO² and diskAshur DT incorporate a secure microprocessor with no debug ports, essentially preventing attackers from modifying the firmware}}.

For example, a hacking company in China, Golon International (http://www.golon.net/), has listed on their website numerous microprocessors which they claim to have hacked. As an example, the Microchip PIC18F26K22 (http://www.golon.net/decrypt?keywords=PIC18F26K22), which is used within some so-called secure portable data storage devices is listed as being hacked. Whereas the same company attempted to hack the iStorage secure microprocessor and failed. We strongly recommend that customers ask manufacturers of secure portable data storage devices to disclose which microprocessor is incorporated within their products, and then visit the Golon website to see if such microprocessors are listed as being hacked. If they are, then we strongly recommend that customers steer clear of any products that incorporate such vulnerable microprocessors.

This latest vulnerability with Self Encrypting SSDs is an excellent example of why PIN authenticated portable data storage devices such as iStorage products, which incorporate secure microprocessors, should be chosen over simple password-based and other PIN authenticated drives that use non-secure microprocessors."

Continues John:

"Aside from this, our customers should be reminded that iStorage drives have passed government security accreditations – where we have products which are certified to FIPS 140-2 Level 2/3, NCSC CPA, NLNCSA BSPA & NATO Restricted Level, all of which have successfully gone through the toughest testing standards and makes iStorage the world's first and only company to have all such certifications."

Any customers who are concerned with whether their drive is secure or not should contact the manufacturer, however iStorage customers can rest assured that their data is secure if saved on iStorage encrypted data storage drives.

For more information or if you would like to request a free 30-day evaluation, please contact evaluation@istorage-uk.com. To find out how the iStorage range can help protect your organisation's confidential data, whilst ensuring GDPR compliance, please visit www.istorage-uk.com (https://istorage-uk.com/) or contact +44 (0) 20 8991 6260.

End.

For more information or to request images or samples for review, please email Holli Cheung at holli.cheung@istorage-uk.com or telephone T: +44 (0)20 8991 6286

About iStorage Limited:
iStorage is the trusted global leader of award winning PIN authenticated, hardware encrypted data storage devices. Delivering the most innovative products to securely store and protect data to military specified encryption levels; safeguarding valuable business information whilst ensuring compliance to regulations and directives.

Industry Awards won: 2013 UK IT Industry Awards Winner, 2015 UK IT Industry Awards Winner, Computing Security Excellence 2016 Awards SME Solution Award Winner, 2017 UK IT Industry Awards - Highly Commended, PC PRO Security Product of the Year 2017 for diskAshur PRO² and 2018 Security Today Magazine New Product of the Year – Winner in the Tools and Hardware Category.
iStorage is also featured on The Hiscox Sunday Times Tech Track 100 2016 List of Britain's fastest growing tech companies, FT 1000 Europe's Fastest Growing Companies 2017, London Stock Exchange Group's 1000 companies to Inspire Britain 2018 and 2018 FT Future 100 UK list of the fast-growing businesses that are shaping the future of their sector and making positive impact on business and society.