DataVault Lite Software Update

Product Line: DataVault and derivatives

Published: 15-12-2021

Last Updated:

Publication issued by: ENC Security

Description

DataVault and its derivatives were using a one-way cryptographic hash with a predictable salt making it vulnerable to dictionary attacks by a malicious user. The software also made use of a password hash with insufficient computational effort that would allow an attacker to brute force user passwords leading to unauthorized access to user data.

Both the key derivation function issues described above have been resolved in the new update.

We urge our customers to install this software update immediately to keep their vaults secure. As with any upgrade, it is best to back up your data before installing the upgrade. Back up your data using the built-in Backup function in the Tools menu. After updating, we recommend users to change their password and to create a new Vault.

For complete instructions on how to upgrade please see:
https://www.sony.net/Products/memorycard/en_us/ssd/software2/encdvlupgrade.pdf

Advisory Summary

The key derivation function issues have been addressed by using PBKDF2-SHA256 together with a randomly generated salt.

CVE Number: CVE-2021-36750

On behalf of all partners, ENC Security would like to thank Sylvain Pelissier for reporting this issue.