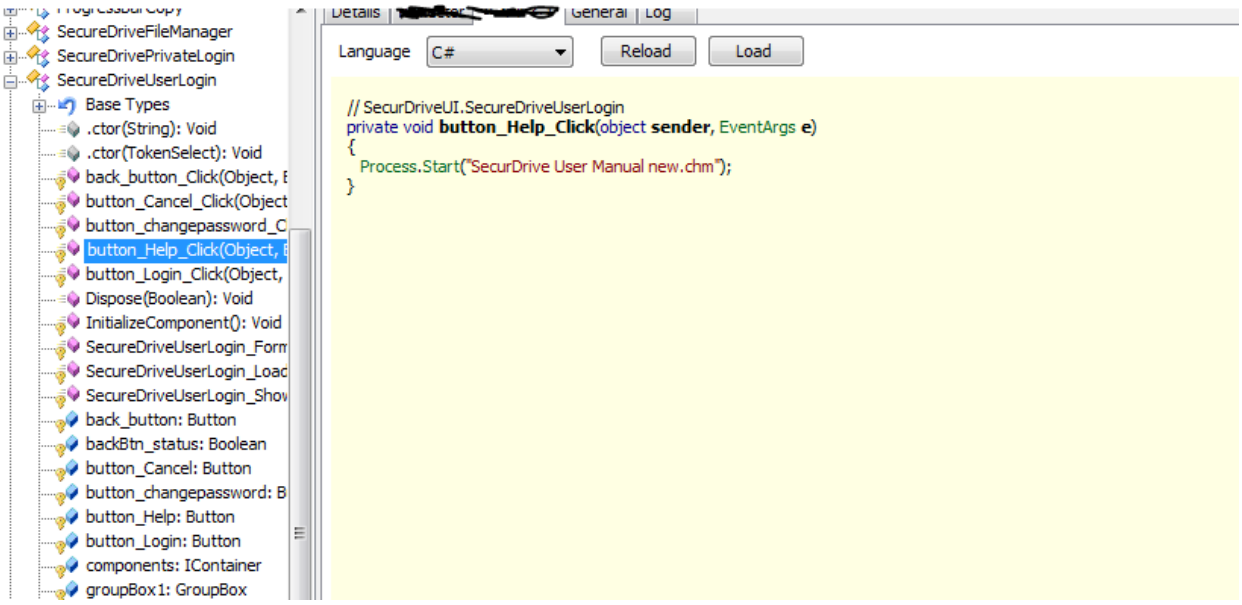
Genisis securedrive is claimed by company to have been coded by IIT delhi. The product is a hardware gemalto based encrypted USB. The company claims to sold to various government sensitive departments and some banks. We tested this product.

- **We found we can decrypt all files without the PIN and password.**
- **The encryption is AES and the key is inside the database on the USB(one partition)**
- **The software code never uses the hardware encryption, its only to show. We removed the hardware encryption chip and we could decrypt the files.**
- **We could change the pin/password without hardware encryption chip.**
- **The software code is full of buffer overflow and we can attack software direcly to get access. The code is written by amateur.**

We recommend not to use this securedrive for storing anything sensitive. We are releasing this in interest of nation/end user people who use it.

Technical report(code exceptions and buffer overflow for techies)

1. **Runtime Check Error : For thrown exceptions there is no Catch statement to handle the runtime errors . It can be removed by declaring a Global class to handle the error like below :**



2. ***Stack memory around allocation was corrupted ->** Stack is like collection of variables which stores data . Stack gets corrupted when it's content exceeds their defined data size.

3. A local variable was used before it was initialized -> It causes runtime errors in the program.

4. Data type definition used was small which caused loss of data. -> For example, if you declare a variable of type int, the compiler allows you to use the variable in addition and subtraction operations. If you try to perform those same operations on a variable of type bool, the compiler generates an error, as shown in the following example:

5.Masking the source of the cast with the appropriate bitmask : (Unappropriate bitmask of char causes vulnerability)

Example: char c = (i & 0xFF); <<-- Changing the code in this way will not affect the quality of resulting optimized code

6. Client side Exeption Error in the main program . (Critical Vulnerability) :
Secure File -> User Login Form (Here Help button has no exception handling which leaks sensitive information about the program .This exception can easily be exploited to open Encrypted files with Loging into the program . Also it's so much vulnerable that if USB Theft occurs or unauthorized access is given to USB then it can be exploited to Log all data or Upload the plain/Unecrypted format of Data to any FTP Server by direct modification in the program) .