

High bosslabdcu published GHSA-j3f7-346q-97f4 on Sep 1, 2021

not patched

Secure External Hard Disk (Samsung H3) Malicious Access Vulnerability

Samsung Drive Manager V2.0.104

The abuse of the disk management function allows an attacker, who has obtained an administrator privilege, to delete or add disks using this vulnerability. In stealing the user's confidential data, the attacker is authenticated as a legitimate user by the exposed password using this vulnerability; hence, the data stored securely inside the disk can be stolen without stealing the decryption key.

Security technologies for external hard disk, such as Secure External Hard Disk, have emerged to prevent the exposure of the data stored inside the disk. These security technologies include user authentication and access control technologies, and user authentication technologies among them are primarily used. Password-based authentication techniques are most used in user authentication technologies for ease of implementation and deployment. For this reason, we selected Samsung Secure External Hard Disk, one of the most used secure external disks, to analyze the vulnerability of the password authentication method applied to the product.

The vulnerability analysis results are showed that attackers who do not have access to a secure disk elevates themselves to an administrator privilege to exploit all the features provided by the secure disk by maliciously stealing user credentials without any additional information.

Analysis

The method applied to Secure External Hard Disk, which is the analysis target, entails the input password being transmitted to the Authentication Module that compares the registered password with the input password. Therefore, the vulnerabilities of the existing password authentication technology, such as the hard-coded password vulnerability in which the password is exposed in the source code as it is, do not exist. However, in the case of Samsung Drive Manager, the password stored in the source code is not only exposed as it is, but also the password is stored in plain text without being encrypted. Consequently, attackers absolutely steal user's password in plain text.

Considering the vulnerability of password authentication through the aforesaid vulnerability analysis results, the user-inputted widechar-type password is converted to multibyte type and compared with the registered password. Therefore, we mainly analyzed the WideCharToMultiByte function to analyze the inputted widechar-type password after conversion. A total of eight parameters were used when calling the WideCharToMultiByte function, and important parameters among them were stored in WideCharStr and MultiByteStr parameters. WideCharStr stores the data before the conversion to multibyte, which is the inputted password, and MultiByteStr stores the address of the inputted password after the conversion.

Thus, the analysis of the address where MultiByteStr data is stored confirmed that the registration password is exposed as shown in the below figure, resulting in a malicious access vulnerability based on the exposed password.

- Registered password: boss.lab.dcu
- Inputted password: testtest

```

01F0F8CDE 546F75B5 CALL to WideCharToMultiByte from SZ,546F75B3
01F0F8CD0 00000000 CodePage = CP_RCP
01F0F8CD4 00000000 Opt Lons = 0
01F0F8CD8 0725E580 WideCharStr = "testtest"
01F0F8CCC FFFFFFFF WideCharCount = FFFFFFFF (-1,)
01F0F8CD0 0725DC48 MultiByteStr = 0725DC48
01F0F8CD4 00000010 MultiByteCount = 10 (16,)
01F0F8CD8 00000000 pDefaultChar = NULL
01F0F8CDC 00000000 pDefaultCharUsed = NULL
01F0F8CE0 7B904C40
01F0F8CE4 00000111
01F0F8CE8 072411A0
01F0F8CEC 54894900 SZ,54894900
01F0F8CF0 54894900 SZ,54894900
01F0F8CF4 0725E580 UNICODE "testtest"
01F0F8CF8 0724D608 UNICODE "Samsung SecretZone"
01F0F8CFC 0725C388 UNICODE "Z1"
01F0F8D00 54894900 SZ,54894900
01F0F8D04 01F0F8D04 Pointer to next SEH record

```

The screenshot shows the Windows Task Manager Performance tab. The 'Memory' section is active, displaying a 'Physical Memory' bar at 100% usage. The bar is highlighted with a red rectangle. Below the bar, the text 'Physical Memory' is visible. The overall system memory usage is 100%.

Discoverer(s)/Credits

Kyungroul Lee/South Korea/carpedm@mnu.ac.kr
Jae hyuk Lee/south korea/gurmggg@cu.ac.kr

Severity

High 8.4 / 10

CVSS base metrics	
Attack vector	Local
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High

CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVE ID

CVE-2021-39373

Weaknesses

CWE-259CWE-262CWE-311

Credits

jh1113