Secure External Hard Disk (Samsung H3) Malicious Access Vulnerability

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

Package

Samsung Drive Manager (Software)

Affected versions

V2.0.104

Patched versions

not patched

Description

Secure External Hard Disk (Samsung H3) Malicious Access Vulnerability

Target

Samsung Drive Manager V2.0.104

Impact

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.

Summary

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

Analysis

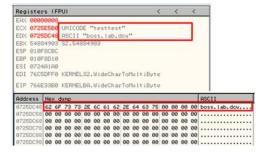
The method applied to Secure External Hard Disk, which is the analysis target, entails the input password being transmitted to the Authentication Module that compares the registered password with the input password. Therefore, the vulnerabilities of the existing password authentication technology, such 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 aforedescribed 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 be address of the inputted password after 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.

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





Discoverer(s)/Credits

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

Severity



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-259 CWE-262 CWE-311

Credits

