CVE-2020-11005

Published on: 04/14/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:25 PM UTC

CVE-2020-11005 - advisory for GHSA-wvpv-ffcv-r6cw

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF

Certain versions of Windowshello from Windowshello Project contain the following vulnerability:

The WindowsHello open source library (NuGet HaemmerElectronics.SeppPenner.WindowsHello), before version 1.0.4, has a vulnerability where encrypted data could potentially be decrypted without needing authentication. If the library is used to encrypt text and write the output to a txt file, another executable could be able to decrypt the text using the static method NCryptDecrypt from this same library without the need to use Windows Hello Authentication again. This has been patched in version 1.0.4.

CVE-2020-11005 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **SeppPenner** - **WindowsHello** version **< 1.0.4**

CVSS3 Score: 5.5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: 2.1 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
[Question] Security of the Encrypted data · Issue #3 · SeppPenner/WindowsHello · GitHub	Issue Tracking Third Party Advisory github.com text/html	MISC github.com/SeppPenner/WindowsHello/issues/3
Internal NCryptDecrypt method could be used by other libraries as well. · Advisory · SeppPenner/WindowsHello · GitHub	Third Party Advisory github.com text/html	CONFIRM github.com/SeppPenner/WindowsHello/security/advisories/GHSA-wvpv-ffcv-r6cw

Related QID Numbers

983126 Dotnet (nuget) Security Update for HaemmerElectronics.SeppPenner.WindowsHello (GHSA-wvpv-ffcv-r6cw)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Windowshello Project	Windowshello	All	All	All	All
Application	Windowshello Project	Windowshello	All	All	All	All

cpe:2.3:a:windowshello_project:windowshello:*:*:*:*:*:*:*:*:

cpe:2.3:a:windowshello_project:windowshello:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→