README.md

CVE_Assessments_11_2019

1Password

A DLL hijacking vulnerability exists in the 1Password version 7.3.712 which could allow an attacker to execute arbitrary code.

File Information: 1password.dll

MD5: 4CF2AC245B8BEA3AA82B4D99891D7925

SHA1: D4AF2E282D9E25BB3C48F61AA6CC5458542F3E70

SAH256: 788FF31C504B579CA9F4B1918397D78613912FE0CE8475F23102A56E27B74CB8

SHA384: 2EEE32B20AC7D41E1227802DC5D5EA05E99BA01803E15889387EECF5C4D69BE08FF1F2AA07BB20FACA948A677FD0B680

SHA512:
C42BB47DC5B064145C9E7692F675D1B2105A31B664B19BB30217620009475C3B5A45886925F80D9E0662647C88F2B0EA8FB5F87D92ACC24717F6E5ABC8443E72

Reference:

https://www.virustotal.com/gui/file/788ff31c504b579ca9f4b1918397d78613912fe0ce8475f23102a56e27b74cb8/details

Examination of the DLL structure

[*] Siofra version 1.13 has entered architecture mode Wow64

======== C:\Program Files (x86)\1Password\app\7\1Password.dll [32-bit PE] ========

1Password.dll

```
ole32.dll [KnownDLL]
    api-ms-win-crt-string-l1-1-0.dll [API set]
        ucrtbase.dll [Base]
    RPCRT4.dll [KnownDLL]
        api-ms-win-core-heap-obsolete-l1-1-0.dll [API set]
            kernel32.dll [KnownDLL]
        SspiCli.dll [Base]
            CRYPTBASE.dll [Base]
                bcryptPrimitives.dll [Base]
    api-ms-win-core-com-midlproxystub-l1-1-0.dll [API set]
        combase.dll [KnownDLL]
    GDI32.dll [KnownDLL]
        api-ms-win-gdi-internal-uap-l1-1-0.dll [API set]
            gdi32full.dll [Base]
                msvcp_win.dll [Base]
                USER32.dll [KnownDLL]
                    win32u.dll [Base]
    api-ms-win-service-management-l1-1-0.dll [API set]
        sechost.dll [KnownDLL]
WS2_32.dll [KnownDLL]
```

```
ADVAPI32.dll [KnownDLL]
    msvcrt.dll [KnownDLL]
bcrypt.dll [!]
CRYPT32.dll [Base]
    MSASN1.dll [Base]
Secur32.dll [!]
SHELL32.dll [KnownDLL]
    api-ms-win-shcore-path-l1-1-0.dll [API set]
        shcore.dll [KnownDLL]
    api-ms-win-storage-exports-internal-l1-1-0.dll [API set]
        windows.storage.dll [Base]
            api-ms-win-shlwapi-winrt-storage-l1-1-1.dll [API set]
                shlwapi.dll [KnownDLL]
            api-ms-win-appmodel-state-l1-2-0.dll [API set]
                kernel.appcore.dll [Base]
            profapi.dll [Base]
            api-ms-win-power-base-l1-1-0.dll [API set]
                powrprof.dll [Base]
            FLTLIB.DLL [Base]
VERSION.dll [!]
wer.dll [!]
WINHTTP.dll [!]
```

[!] Module bcrypt.dll vulnerable at C:\Program Files (x86)\1Password\app\7\bcrypt.dll (real path: C:\Windows\SysWOW64\bcrypt.dll)

[!] Module Secur32.dll vulnerable at C:\Program Files (x86)\1Password\app\7\Secur32.dll (real path: C:\Windows\SysWOW64\Secur32.dll)

[!] Module VERSION.dll vulnerable at C:\Program Files (x86)\1Password\app\7\VERSION.dll (real path: C:\Windows\SysWOW64\VERSION.dll)

[!] Module wer.dll vulnerable at C:\Program Files (x86)\1Password\app\7\wer.dll (real path: C:\Windows\SysWOW64\wer.dll)

[!] Module WINHTTP.dll vulnerable at C:\Program Files (x86)\1Password\app\7\WINHTTP.dll (real path: C:\Windows\SysWOW64\WINHTTP.dll)

Releases

No releases published

Packages

No packages published