exploits-forsale / themebleed Public

Notifications Fork 38 Star 186

Code Issues 2 Pull requests Actions Projects Security Insights

main Go to file Code

gabe-k Create README.md 6e519df · last year 3 Commits

SMBFilterDemo	initial commit	last year
data	added binary stage files	last year
README.md	Create README.md	last year
ThemeBleed.sln	initial commit	last year

README

ThemeBleed

Proof-of-Concept for CVE-2023-38146 ("ThemeBleed")

```
Usage: ThemeBleed.exe <command>

Commands:
        server                                  - Runs the server
        make_theme <host> <output path>         - Generates a .theme
        make_themepack <host> <output_path>     - Generates a .theme
```

Data files

The binaries in data correspond to the 3 files returned to the target by the PoC.

- `stage_1` - An `msstyles` file with the `PACKTHEM_VERSION` set to 999.
- `stage_2` - A valid unmodified `msstyles` file to pass the signature check.
- `stage_3` - The DLL that will be loaded and executed. The provided example simply launches `calc.exe`.

To make your own payload, create a DLL with an export named `VerifyThemeVersion` containing your code, and replace `stage_3` with your newly created DLL.

About

Proof-of-Concept for CVE-2023-38146 ("ThemeBleed")

Readme
Activity
Custom properties
186 stars
4 watching
38 forks
Report repository

Releases 1

ThemeBleed PoC Latest
on Sep 13, 2023

Packages

No packages published

Languages

C# 100.0%