

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.

Terms Privacy Security Status Docs Contact Manage cookies Do not share my personal information © 2024 GitHub, Inc.