

Disabling the EFS service seems not to mitigate the "feature"

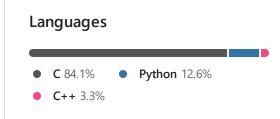
The Python one require Impacket to be installed, the Windows PoC was done on VS 2019 Community. If compilation problem, remember to add Rpcrt4.lib in the linker. Compile in x86.

Inspired by the previous work on MS-RPRN from @tifkin_ & @elad_shamir and others SpecterOps guys.

Incomplete patch from Microsoft :)
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36942

MS-EFSRPC - Encrypting File System Remote (EFSRPC)
Protocol https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-efsr/08796ba8-01c8-4872-9221-1000ec2eff31





Terms Privacy Security Status Docs Contact Manage cookies Do not share my personal information