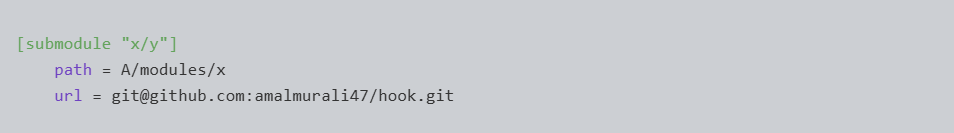
**git의 원격 코드 실행 취약점**

버전 관리 시스템인 git의 clone 기능에서 발견된 원격 코드 실행 취약점의 세부 정보가 공개되었습니다.

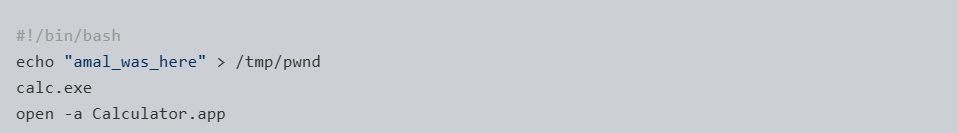
git clone 기능은 저장소에 포함된 하위 모듈을 재귀적으로 함께 clone하는 --recurse-submodules 옵션이 존재합니다. 또한 git은 symbolic link를 지원하여 git 컨텍스트에서 저장소의 다른 부분을 참조하는데 사용할 수 있습니다.

취약점은 대소문자를 구분하지 않는 Windows, MacOS와 같은 파일 시스템에서 --recurse-submodules 옵션을 사용해 저장소를 clone하는 과정에서 발견되었습니다.

하위모듈 경로는 일반적으로 .gitmodules 파일에 다음과 같이 작성됩니다.



해당 하위모듈 url은 https://github.com/amalmurali47/hook 저장소를 가리키며 해당 저장소의 hook/post-checkout hook script는 실행할 임의 코드가 작성되어 있습니다.



위 PoC는 https://github.com/amalmurali47/git\_rce 에서 확인할 수 있습니다.

대소문자를 구분하지 않는 파일시스템은 A/modules/x 및 a/modules/x 와 같은 경로를 동일하게 인식합니다. 이를 이용하면 다음과 같은 exploit이 가능합니다

1. clone 대상 저장소 git\_rce에 .git을 가리키는 symbolic link a 생성
2. 해당 저장소를 recurse clone하면 git은 .gitmodules에 정의된 대로 하위 모듈용 디렉토리 A/modules/x를 생성해 해당 경로에 clone하려고 시도함
3. 그러나 대소문자를 구분하지 않는 파일시스템은 2번의 경로를 symbolic link인 a의 하위 경로 a/modules/x 로 인식함.
4. a는 .git 을 가리키므로 원격 저장소의 hook/post-checkout hook script가 로컬 하위 모듈의 .git/hook/post-checkout에 생성됨
5. 해당 hook script는 checkout 성공 이후 자동으로 트리거되어 임의 코드 실행이 가능함

해당 취약점은 symbolic link를 지원하는 core.symlinks 기능이 활성화된 Windows 및 MacOS 시스템이 취약하며, 패치는 커밋 링크에서 확인할 수 있습니다.

원문링크

https://hackyboiz.github.io/2024/05/19/l0ch/2024-05-19/