# CVE Detail – CVE-2023-25815

In Git for Windows, the Windows port of Git, no localized messages are shipped with the installer. As a consequence, Git is expected not to localize messages at all, and skips the gettext initialization. However, due to a change in MINGW-packages, the `gettext()` function's implicit initialization no longer uses the runtime prefix but uses the hard-coded path `C:\mingw64\share\locale` to look for localized messages. And since any authenticated user has the permission to create folders in `C:\` (and since `C:\mingw64` does not typically exist), it is possible for low-privilege users to place fake messages in that location where `git.exe` will pick them up in version 2.40.1.  
  
This vulnerability is relatively hard to exploit and requires social engineering. For example, a legitimate message at the end of a clone could be maliciously modified to ask the user to direct their web browser to a malicious website, and the user might think that the message comes from Git and is legitimate. It does require local write access by the attacker, though, which makes this attack vector less likely. Version 2.40.1 contains a patch for this issue. Some workarounds are available. Do not work on a Windows machine with shared accounts, or alternatively create a `C:\mingw64` folder and leave it empty. Users who have administrative rights may remove the permission to create folders in `C:\`.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.26965

## CVSS Scoring

CVSS v3.1 Score: 3.3

Severity: LOW

## Mapped CWE(s)

* CWE-134: Use of Externally-Controlled Format String
* CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

## CAPEC(s)

* CAPEC-126: Path Traversal
* CAPEC-135: Format String Injection
* CAPEC-64: Using Slashes and URL Encoding Combined to Bypass Validation Logic
* CAPEC-67: String Format Overflow in syslog()
* CAPEC-76: Manipulating Web Input to File System Calls
* CAPEC-78: Using Escaped Slashes in Alternate Encoding
* CAPEC-79: Using Slashes in Alternate Encoding

## Affected Products

* cpe:2.3:a:git\_for\_windows\_project:git\_for\_windows:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:37:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:38:\*:\*:\*:\*:\*:\*:\*