



CVE-2020-26233

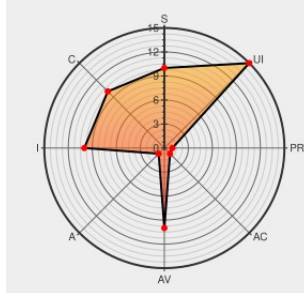
Published on: 12/08/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:56 PM UTC

CVE-2020-26233 - advisory for GHSA-2gg7-ww4j-3m76

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:N



Certain versions of [Git Credential Manager Core](#) from [Microsoft](#) contain the following vulnerability:

Git Credential Manager Core (GCM Core) is a secure Git credential helper built on .NET Core that runs on Windows and macOS. In Git Credential Manager Core before version 2.0.289, when recursively cloning a Git repository on Windows with submodules, Git will first clone the top-level repository and then recursively clone all

submodules by starting new Git processes from the top-level working directory. If a malicious git.exe executable is present in the top-level repository then this binary will be started by Git Credential Manager Core when attempting to read configuration, and not git.exe as found on the %PATH%. This only affects GCM Core on Windows, not macOS or Linux-based distributions. GCM Core version 2.0.289 contains the fix for this vulnerability, and is available from the project's GitHub releases page. GCM Core 2.0.289 is also bundled in the latest Git for Windows release; version 2.29.2(3). As a workaround, users should avoid recursively cloning untrusted repositories with the --recurse-submodules option.

CVE-2020-26233 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **microsoft - Git-Credential-Manager-Core** version <= 2.0.280

CVSS3 Score: **7.3 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	HIGH	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	HIGH	HIGH	NONE

CVSS2 Score: **3.6 - LOW**

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	SINGLE

NETWORK	HIGH	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
Attack of the clones 2: Git CLI remote code execution strikes back	Exploit Third Party Advisory blog.blazeinfosec.com text/html	 MISC blog.blazeinfosec.com/attack-of-the-clones-2-git-command-client-remote-code-execution-strikes-back/
Merged PR 585167: [Security] Enumerate the PATH environment variable ... · microsoft/Git-Credential-Manager-Core@61c0388 · GitHub	Patch Third Party Advisory github.com text/html	 MISC github.com/microsoft/Git-Credential-Manager-Core/commit/61c0388e064babb3b4e60d3ec269e8a07ab3bc76
Git recursive clone can result in remote code execution facilitated by GCM Core (affects Windows only) · Advisory · microsoft/Git-Credential-Manager-Core · GitHub	Third Party Advisory github.com text/html	 CONFIRM github.com/microsoft/Git-Credential-Manager-Core/security/advisories/GHSA-2gq7-ww4j-3m76
git-clone(1) Manual Page	Third Party Advisory git-scm.com text/html	 MISC git-scm.com/docs/git-clone#Documentation/git-clone.txt---recurse-submodules!pathspeccgt
Release GCM 2.0.289-beta · microsoft/Git-Credential-Manager-Core · GitHub	Release Notes Third Party Advisory github.com text/html	 MISC github.com/microsoft/Git-Credential-Manager-Core/releases/tag/v2.0.289-beta

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

[375469](#) Git Credential Manager Core Untrusted Cloning of Repository Vulnerability

[375543](#) Git Credential Manager Core Untrusted Cloning of Repository Vulnerability

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Git Credential Manager Core	All	All	All	All
Application	Microsoft	Git Credential Manager Core	All	All	All	All
cpe:2.3:a:microsoft:git_credential_manager_core:*****:windows:***:						
cpe:2.3:a:microsoft:git_credential_manager_core:*****:windows:***:						

No vendor comments have been submitted for this CVE

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)