



CVE-2023-29011

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2023-29011
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-04-25 21:15:00 UTC
Updated	2023-05-04 21:18:00 UTC
Description	Git for Windows, the Windows port of Git, ships with an executable called `connect.exe`, which implements a SOCKS5 pro

Risk And Classification

Problem Types: CWE-427

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Git For Windows Project	Git For Windows	All	All	All	All

References

Reference	Source	Link	Tags
The config file of `connect.exe` is susceptible to malicious placing · Advisory · git-for-windows/git · GitHub	MISC	github.com	
Release Git for Windows 2.40.1 · git-for-windows/git · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	cano
NVD vulnerability detail	NVD	nvd.nist.gov	cano

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[378458](#) Git for Windows Multiple Security Vulnerability

[378588](#) Microsoft Edge Based on Chromium Prior to 109.0.1518.115 Multiple Vulnerabilities

[92027](#) Microsoft Visual Studio Security Updates for June 2023

© [CVE.report](#) 2026 |

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](#)