



CVE-2026-5160

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

Summary

CVE	CVE-2026-5160
State	PUBLISHED
Assigner	snyk
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-15 06:16:13 UTC
Updated	2026-04-17 15:17:00 UTC
Description	Versions of the package github.com/yuin/goldmark/renderer/html before 1.7.17 are vulnerable to Cross-site Scripting (XSS)

Risk And Classification

Primary CVSS: v4.0 5.1 MEDIUM from report@snyk.io

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:L/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000390000 probability, percentile 0.118180000 (date 2026-04-21)

Problem Types: CWE-79 | CWE-79 Cross-site Scripting (XSS)

Version	Source	Type	Score	Severity	Vector
4.0	report@snyk.io	Secondary	5.1	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:L/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
4.0	CNA	DECLARED	5.1	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:L/SI:L/SA:N
3.1	report@snyk.io	Secondary	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/L/I:L/A:N
3.1	CNA	DECLARED	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/L/I:L/A:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

security.snyk.io/vuln/SNYK-GOLANG-GITHUBCOMYUINGOLDMARKRENDERERHTML-15838406	report@snyk.io	security.snyk.io	
github.com/yuin/goldmark/commit/cb46bbc4eca29d55aa9721e04ad207c23ccc44f9	report@snyk.io	github.com	
CVE Program record	CVE.ORG	www.cve.org	car
NVD vulnerability detail	NVD	nvd.nist.gov	car

Vendor Comments And Credit

Discovery Credit

CNA: Catalin Iovita (Snyk Security Research) (en)

There are currently no legacy QID mappings associated with this CVE.

© [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](#).

Free CVE JSON API [cve.report/api](#)

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