



Unauthenticated RCE in DocsGPT MCP STUDIO Configuration

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary

CVE	CVE-2026-26015
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-29 18:16:03 UTC
Updated	2026-05-06 20:16:31 UTC
Description	DocsGPT is a GPT-powered chat for documentation. From version 0.15.0 to before version 0.16.0, an attacker accessing b

Risk And Classification

Primary CVSS: v4.0 10 CRITICAL from security-advisories@github.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/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: 0.002830000 probability, percentile 0.516160000 (date 2026-05-05)

Problem Types: CWE-77 | CWE-77 CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	10	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H
4.0	CNA	DECLARED	10	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/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



CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Arc53	Docsgpt	0.15.0	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
--------	--------	---------	---------	-----------

Source	Vendor	Product	Version	Platform
CNA	Arc53	DocsGPT	affected >= 0.15.0, < 0.16.0	Not specified
References				
Reference	Source		Link	
www.ox.security/blog/the-mother-of-all-ai-supply-chains-critical-systemic-vul...	af854a3a-2127-422b-91ae-364da2661108		www.ox.secu	
github.com/arc53/DocsGPT/releases/tag/0.16.0	security-advisories@github.com		github.com	
www.ox.security/blog/mcp-supply-chain-advisory-rce-vulnerabilities-across-the...	af854a3a-2127-422b-91ae-364da2661108		www.ox.secu	
github.com/arc53/DocsGPT/security/advisories/GHSA-gcrq-f296-2j74	134c704f-9b21-4f2e-91b3-4a467353bcc0		github.com	
CVE Program record	CVE.ORG		www.cve.org	
NVD vulnerability detail	NVD		nvd.nist.gov	
No vendor comments have been submitted for this CVE.				
There are currently no legacy QID mappings associated with this CVE.				