Remote code execution via JavaScript injection in `BrowserAutomation::PlaywrightService`

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-41512
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-08 14:16:34 UTC
Updated	2026-05-11 17:20:02 UTC
Description	ai-scanner is an AI model safety scanner built on NVIDIA garak. From version 1.0.0 to before version 1.4.1, there is a remo

Risk And Classification

Primary CVSS: v3.1 9.9 CRITICAL from security-advisories@github.com

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

EPSS: 0.002870000 probability, percentile 0.521100000 (date 2026-05-12)

Problem Types: CWE-94 | CWE-94 CWE-94: Improper Control of Generation of Code ('Code Injection')

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	9.9	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
3.1	CNA	DECLARED	9.9	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

High

ntegrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mozilla	0din Scanner	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	0din-ai	Ai-scanner	affected >= 1.0.0, < 1.4.1	Not specified

References

Reference	Source	Link	Tags
github.com/0din-ai/ai-scanner/security/advisories/GHSA-r27j-xxgx-f5vr	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com	Exploit, V
github.com/0din-ai/ai-scanner/releases/tag/v1.4.1	security-advisories@github.com	github.com	Patch, Pr
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica

No vendor comments have been submitted for this CVE.

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