



# CAPTCHA - Moderately critical - Access bypass - SA-CONTRIB-2026-015

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

## Summary

<b>CVE</b>	CVE-2026-3214
<b>State</b>	PUBLISHED
<b>Assigner</b>	drupal
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-25 16:16:22 UTC
<b>Updated</b>	2026-04-02 20:36:11 UTC
<b>Description</b>	Authentication Bypass Using an Alternate Path or Channel vulnerability in Drupal CAPTCHA allows Functionality Bypass. TI

## Risk And Classification

**Primary CVSS:** v3.1 6.5 MEDIUM from ADP

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

**Problem Types:** CWE-288 | CWE-288 CWE-288 Authentication Bypass Using an Alternate Path or Channel

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

## CVSS v3.1 Breakdown

Attack Vector

**Network**

Attack Complexity

**Low**

Privileges Required

**None**

User Interaction

**None**

Scope

**Unchanged**

Confidentiality

**Low**

Integrity

Low

Availability

None

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Arnabdotorg</a>	<a href="#">Captcha</a>	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Drupal</a>	<a href="#">CAPTCHA</a>	affected 0.0.0 1.17.0 semver	Not specified
CNA	<a href="#">Drupal</a>	<a href="#">CAPTCHA</a>	affected 2.0.0 2.0.10 semver	Not specified

### References

Reference	Source	Link	Tags
<a href="#">www.drupal.org/sa-contrib-2026-015</a>	<a href="mailto:mlhess@drupal.org">mlhess@drupal.org</a>	<a href="http://www.drupal.org">www.drupal.org</a>	Vendor Advisory
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

### Vendor Comments And Credit

Discovery Credit

**CNA:** Andrew Wang ([andrew.wang](#)) (en)

**CNA:** Andrew Belcher ([andrewbelcher](#)) (en)

**CNA:** Chris Dudley ([dudleyc](#)) (en)

**CNA:** M Parker ([mparker17](#)) (en)

**CNA:** [tamasd](#) (en)

**CNA:** Tim Wood ([timwood](#)) (en)

**CNA:** Denis K\*\*\*\* ([dench0](#)) (en)

**CNA:** Joshua Sedler ([grevil](#)) (en)

**CNA:** Jakob P ([japerry](#)) (en)

**CNA:** Adam Nagy ([joevagyok](#)) (en)

**CNA:** [cilefen](#) ([cilefen](#)) (en)

**CNA:** Damien McKenna ([damienmckenna](#)) (en)

**CNA:** Greg Knaddison (greggles) (en)

**CNA:** Lee Rowlands (larowlan) (en)

**CNA:** Michael Hess (mlhess) (en)

**CNA:** Juraj Nemec (poker10) (en)

**CNA:** Jess (xjm) (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](#)