contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Drupal Core exploited

CVE-2026-132165 · on CISA's exploited list since 24 November 2026

Analysis Report

Any Drupal Core site on a version below 10.6.22, 11.3.22, or 11.4.13 must patch by 27 November 2026 — if you do not run Drupal, stop here. The vendor's advisory reports exploitation on live sites …

PREPARED BY	NamiQ	DATE	26 November 2026
FACTS AS OF	26 November 2026	VERSION	1.0
SEVERITY	**Not scored yet**	STATUS	On CISA's exploited list; due 27 November 2026

NamiQ © 2026 NamiQ. All rights reserved. This document is the property of NamiQ. It may be shared unaltered, with attribution.
Companion article: namiq.io/insights/drupal-core-cve-2026-132165

The bottom line

> *Any Drupal Core site on a version below 10.6.22, 11.3.22, or 11.4.13 must patch by 27 November 2026 — if you do not run Drupal, stop here. The vendor's advisory reports exploitation on live sites from 19 November 2026; identify your version and patch immediately.*

At a glance

Fact	Detail
Product	Drupal Core (CVE-2026-132165)
Severity	Not scored when we read it
CISA	On its exploited list since 24 November 2026. Deadline for US federal agencies: 27 November 2026.
Chance of exploitation (EPSS)	Not available yet
Ransomware use	Not recorded by CISA. That is not the same as none.
Fixed in	Drupal 10.6.22; Drupal 11.3.22; Drupal 11.4.13 — named as the corrected releases in vendor advisory SA-CORE-2026-017 (18 November 2026).
Who looks first	Any organisation running Drupal Core below 10.6.22 (10.6.x branch), below 11.3.22 (11.3.x), or below 11.4.13 (11.4.x). Drupal 8, 9, 10.5.x and below, and 11.2.x and below are end-of-life and will receive no patch.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run any Drupal Core website, self-hosted or managed?	Nothing to do for this CVE.	Check the Drupal version running on each site.
Is any site on a version below 10.6.22, below 11.3.22 (11.3.x), or below 11.4.13 (11.4.x)?	Not in the affected range; no action needed.	Patch immediately — the vendor reports active exploitation.
Can install.php be reached by unauthenticated visitors on those affected sites?	Some exploit paths may be reduced; patching is still required.	Treat as urgent; also secure the installer while patching.

Is Drupal Steward active on the affected sites?	No network-layer protection in place; patch without delay.	Known attack vectors are blocked; the advisory still recommends patching.

What it is

Under specific conditions, an unauthenticated attacker can reach the Drupal installer (install.php) on a live site and use it to attempt to reinstall Drupal, which can result in a full site takeover or the execution of arbitrary code.

Why it matters

The vendor's advisory rates this A:None — no login is required. The exploit metric is E:Exploit, meaning working exploit code was known at disclosure on 18 November 2026. The advisory was updated to note exploitation on live sites from 19 November 2026, one day after disclosure. Our reading is that confirmed exploitation within a day of the advisory means the patch window is effectively closed for any site still exposed.

What the vendor's advisory says

We read one page on www.drupal.org. In short:

- SA-CORE-2026-017, rated 20/25 Highly critical (AC:Complex/A:None/CI:All/II:All/E:Exploit/TD:Uncommon). This advisory covers a single CVE.
- The advisory was updated to note exploitation on live sites was reported from 19 November 2026 at 19:00 UTC.
- Workaround: the advisory instructs securing the Drupal installer, which mitigates some but not all exploit paths.
- Drupal Steward is stated to protect against known attack vectors; the advisory says sites should still patch in case additional attack vectors are discovered.
- Drupal 11.2.x and below, 10.5.x and below, Drupal 8 and 9 are end-of-life and do not receive security coverage for this flaw.

Things people will get wrong

- Drupal Steward means no further action is needed. The vendor's advisory says Steward protects from known attack vectors but instructs patching in case additional attack vectors are discovered.
- Restricting install.php fully resolves the exposure. The advisory states that restricting the web server's ability to write to settings.php mitigates some but not all exploit paths; patching is still required.

- End-of-life Drupal versions will receive a backport patch. The advisory explicitly states that Drupal 11.2.x and below, 10.5.x and below, Drupal 8 and 9 are end-of-life and do not receive security coverage for this flaw.

How we would triage it

This is our judgement.

Step 1: Find the Drupal version on each site

- Check the admin panel under Reports → Status report, or ask your host which Drupal Core version is installed.
- Confirm whether the version falls below 10.6.22, 11.3.22, or 11.4.13 — those are the fixed releases named in the vendor's advisory.

Step 2: Secure the installer as a temporary measure

- The vendor's advisory recommends securing the Drupal installer to reduce exposure while the patch is applied; follow the vendor's official instructions for this step.
- This is a mitigation only — the advisory says it blocks some but not all exploit paths.

Step 3: Apply the patch

- Update to Drupal 10.6.22 (10.6.x), 11.3.22 (11.3.x), or 11.4.13 (11.4.x) — the fixed versions named in advisory SA-CORE-2026-017.
- Sites on Drupal 8, 9, 10.5.x and below, or 11.2.x and below receive no patch; the vendor's advisory recommends migration.

Step 4: Check for signs of exploitation

- Review web server access logs for requests to install.php on or after 19 November 2026 — the date the vendor's advisory says exploitation was first reported.
- Check for unexpected admin-level accounts or changes to settings.php after 19 November 2026, as the advisory lists site takeover as a possible outcome.

To close it, read the version from the product itself, not from an old inventory, and save the output with the date. If you cannot update today, write down who owns it, the new date, and what limits exposure until then. CISA's wording adds that you should stop using the product if no mitigation is available.

Send this to your IT provider

Copy it, change the names and dates, and send it. It is a draft for you to check, not a template tested with any provider.

> *We are writing about CVE-2026-132165, a remote code execution flaw in Drupal Core. CISA has listed this with a remediation deadline of 27 November 2026. The vendor reports exploitation on live sites from 19 November 2026. Please confirm: (1) whether we run any Drupal Core sites, and on which versions; (2) whether those versions are below 10.6.22 (Drupal 10.6.x), 11.3.22 (Drupal 11.3.x), or 11.4.13 (Drupal 11.4.x); and (3) whether install.php is accessible to unauthenticated visitors. Please provide written confirmation of the version running and whether the patch has been applied, by 27 November 2026.*

Signs it was used

An update closes the hole. It does not tell you whether someone used it first. CISA's required action points to its forensic triage requirements (BOD 26-04). Look for:

- Review web server access logs for requests to install.php on or after 19 November 2026 — the vendor's advisory identifies that date as the start of confirmed exploitation.
- Check for new admin-level user accounts created after 19 November 2026, as site takeover is stated as a possible outcome of a successful attack.
- Look for unexpected modifications to settings.php after 19 November 2026, as the advisory identifies it as a file an attacker may need to write to.

The weakness behind it

The record classes this as CWE-306.

Likely ATT&CK mapping

MITRE ATT&CK is a public catalogue of the steps attackers take, from getting in to causing damage. No source has mapped this flaw to it yet, so the steps below are our prediction from what the record says the flaw allows. They are not MITRE's, the vendor's or CISA's, and an attacker may do other things.

Steps an attacker would likely take with this flaw

The step, in plain words	Stage of an attack	Why we think so

Exploit Public-Facing Application (T1190): Breaking in through a service that faces the internet, such as a web server, VPN or login page.	Initial Access: getting in	The flaw is in install.php on a network-reachable web application; an unauthenticated attacker would likely reach it over HTTP, fitting an exploit of a public-facing application.
Create Account (T1136): Creating a new account so the attacker can come back later.	Persistence: staying in	The record states a reinstall can result in site takeover; creating a new administrative account would typically follow from forcing a fresh installation.
Command and Scripting Interpreter (T1059): Running commands or scripts on a machine, such as a shell or PowerShell.	Execution: running the attacker's code	Remote code execution is explicitly stated as a possible outcome; execution would likely occur through the web application's server-side scripting environment.

How to use this: ask your IT provider which control or log would show each step, for example whether sign-in attempts from the internet are recorded. If nobody can answer, that is the gap to close first.

MITRE ATT&CK® is a registered trademark of The MITRE Corporation. Technique names are MITRE's.

The sources, in their words

CISA's catalogue entry:

> *Drupal Core contains a not failing securely vulnerability that could allow an unauthenticated attacker to take over an existing site or execute arbitrary code via the Drupal installer. Under specific conditions, the attacker can use install.php to attempt to reinstall Drupal on the site.*

The CVE record, published by Drupal on 26 November 2026:

> *Missing Authentication for Critical Function vulnerability in Drupal Drupal core allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Drupal core versions: from 0.0.0 to 10.6.22, from 11.0.0 to 11.3.22, from 11.4.0 to 11.4.13.*

Versions of Drupal core the record lists as affected:

- 0.0.0 up to, but not including, 10.6.22
- 11.0.0 up to, but not including, 11.3.22
- 11.4.0 up to, but not including, 11.4.13

The affected ranges end before 10.6.22, 11.3.22, 11.4.13. Those are the first versions the record does not list as affected; confirm them in the vendor's advisory.

CISA's required action:

> *Apply mitigations in accordance with vendor instructions.*

Check your own project

If you build software, you can compare what a project declares with this CVE from a terminal. The tool reads requirements files, package.json, Maven, Gradle, Cargo, CMake and Dockerfile files, runs nothing, and only the CVE id leaves your machine. Naming the CVEs needs no key.

```
lattice-scan project . --cve CVE-2026-132165
```

Each row says in-range, outside-range, undetermined or lead, with the file and line. That is evidence about what a manifest declares, not about what runs, and a person decides. The verdicts, the CSV columns and a pipeline recipe are in the guide.

Check the servers you run

The same id can be checked against a host. Run this on the machine itself, not on the laptop that deploys to it: it reads installed packages (dpkg, rpm or apk), snaps, the hardware (maker, model, firmware), the running container images with their operating system and packages, and the kernel version, compares them on the spot, and only the CVE ids leave the machine; the inventory stays on it, in ~/.lattice-scan. Naming the CVEs needs no key. Do it on each server after a deployment, and again when a new entry lands.

```
lattice-scan --cve CVE-2026-132165
```

A match is a candidate for a person to confirm, not a finding. A distribution can fix a CVE under an unchanged version number, so a match is a candidate; on Debian-family hosts the report also shows whether the package's own changelog names the CVE. By default it opens the images your containers are running and reads their operating system and package list; a deep scan (--deep, a few minutes) opens every local image and the Python, Node, Java and Ruby packages inside them; for what an image declares, use the project check on its Dockerfile.

Guide: namiq.io/lattice/guides/choose-your-channel. MCP server (io.namiq/lattice in the MCP registry): namiq.io/lattice. Package: pypi.org/project/lattice-scan, or namiq.io/apt.

What we do not know yet

- The advisory does not specify the exact conditions under which install.php becomes reachable by an attacker, so the full scope of exposure is not public.
- The advisory says restricting write permissions on settings.php mitigates some but not all exploit paths; which paths remain open is not disclosed.
- No standard CVSS base score is recorded; the vendor's advisory uses its own 20/25 scale (Highly critical).
- We have not tested this against any environment. Versions and scores are as the sources state them and as at 26 November 2026; the vendor's advisory wins where it differs.

- The sections headed "The bottom line", "Does this apply to you?", "What it is", "Why it matters", "Exposure by situation", "Things people will get wrong", "Likely ATT&CK mapping", "How we would triage it" and "Send this to your IT provider" are our interpretation of the sources, not a statement by CISA or the vendor.

Appendix 1. Timeline

Date	Event
24 November 2026	CISA added it to its list of exploited vulnerabilities.
26 November 2026	CVE record published by Drupal.
27 November 2026	CISA's deadline for US federal agencies.

Appendix 2. Exposure by situation

These priorities are our judgement from the attacker prerequisites in the sources. They are not vendor ratings.

Your situation	Priority	Timeframe
Drupal site on an affected version with install.php reachable by unauthenticated visitors	High	Before 27 November 2026 — CISA deadline is tomorrow
Drupal site on an affected version, install.php restricted but no Drupal Steward	High	Before 27 November 2026
Drupal site on an affected version with Drupal Steward active	Medium	This week — the advisory recommends patching regardless
Drupal 8, 9, or other end-of-life branch — no patch available from the vendor	High	Immediately — consider migration or taking the site offline
Drupal site already on 10.6.22, 11.3.22, or 11.4.13 or later	None	No action needed for this CVE

Appendix 3. Definition of done

- Every Drupal Core you run is listed, with its version.
- Each is outside the affected list, or the vendor's mitigation is in place.
- The version output or a screenshot is saved with the date.
- Your projects' declared dependencies were checked against this CVE, and every row has a written reason.
- Logs for the weeks before the update were searched, and anything odd was written down.

- Anything not done has an owner and a date.

Sources

- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- CVE record for CVE-2026-132165: https://www.cve.org/CVERecord?id=CVE-2026-132165
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Advisory or release notes read: www.drupal.org/sa-core-2026-017: https://www.drupal.org/sa-core-2026-017