contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Drupal Core exploited

CVE-2026-136716 · on CISA's exploited list since 27 November 2026

Analysis Report

Any organisation running Drupal Core on an affected version should act before 30 November 2026; the vendor's advisory confirms exploitation in the wild. The first step is to confirm whether …

PREPARED BY	NamiQ	DATE	27 November 2026
FACTS AS OF	27 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 3.1 9.8**	STATUS	On CISA's exploited list; due 30 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-2026-136716

The bottom line

> *Any organisation running Drupal Core on an affected version should act before 30 November 2026; the vendor's advisory confirms exploitation in the wild. The first step is to confirm whether install.php is publicly accessible — the advisory says sites with a secured installer are not vulnerable.*

At a glance

Fact	Detail
Product	Drupal Core (CVE-2026-136716)
Severity	Critical: 9.8 (CVSS 3.1)
CISA	On its exploited list since 27 November 2026. Deadline for US federal agencies: 30 November 2026.
Chance of exploitation (EPSS)	0.01, the estimated chance in the next 30 days, as at 27 November 2026
Ransomware use	Not recorded by CISA. That is not the same as none.
Fixed in	Drupal 10.6.23; Drupal 11.3.23; Drupal 11.4.14 (vendor advisory, 25 November 2026). The advisory also requires running update.php after upgrading.
Who looks first	Anyone running Drupal Core before version 10.6.23, or on 11.0–11.3.x before 11.3.23, or 11.4.x before 11.4.14, whose installer is not confirmed as secured.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run Drupal Core on any website or application?	Nothing to do for this CVE.	Check the version you are running.
Is install.php publicly accessible on your Drupal site?	The advisory says secured-installer sites are not vulnerable; patch at next cycle.	Treat the site as potentially compromised; patch and check logs immediately.
Do your logs show unexpected changes to or by the user 1 account?	Patch and run update.php as the advisory directs.	Follow the advisory's guidance for compromised Drupal sites before patching.

What it is

An unauthenticated attacker who can reach Drupal's installer can take over the site entirely if it is in an unusual or incomplete installation state. No login is required.

Why it matters

The record scores this 9.8 on CVSS 3.1. The vendor's advisory confirms exploitation in the wild and notes that sites already compromised may no longer appear vulnerable, making prior exposure hard to rule out from the interface alone. No authentication is needed; the attack path is the installer, reachable over a network. Our reading is that the short CISA window reflects active exploitation and warrants treating any unpatched, installer-exposed site as a priority regardless of apparent install status.

What the vendor's advisory says

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

- SA-CORE-2026-017, issued earlier, fixed several vulnerabilities in the Drupal installer; this advisory addresses sites that remained vulnerable in unusual or incomplete install states after that fix.
- Drupal Steward's recommended mitigations protect both SA-CORE-2026-017 and this issue from known attack vectors, but the advisory says sites should upgrade in case additional attack vectors are discovered.
- After upgrading, the advisory requires running update.php: an update hook must run to fix existing production sites in the affected state.
- Drupal 11.2.x and below and 10.5.x and below are end-of-life and do not receive security coverage. Drupal 8 and 9 are also end-of-life.

Things people will get wrong

- Securing the installer after SA-CORE-2026-017 means this site is now safe The advisory says certain sites in unusual or incomplete states remain vulnerable even after SA-CORE-2026-017, and already-compromised sites may no longer appear vulnerable.
- The site shows as fully installed so it cannot be in the vulnerable state The advisory explicitly says it is not apparent in the user interface whether a site is in the affected state, and that already-compromised sites may no longer appear vulnerable.
- Only sites with an obvious incomplete install are at risk The advisory names production sites as among those that may be in the affected state, and says the condition is not visible in the UI.

How we would triage it

This is our judgement.

Step 1: Check whether the installer is reachable

- Attempt to load install.php from outside the network. If it loads or prompts for installer steps, the file is exposed. The advisory says secured-installer sites are not vulnerable to this flaw.

Step 2: Upgrade to the fixed version and run update.php

- The vendor's advisory names 10.6.23, 11.3.23, and 11.4.14 as the fixed releases. The advisory requires running update.php after upgrading; an update hook must run to fix sites in the affected state.
- Drupal 11.2.x and below and 10.5.x and below are end-of-life; the advisory does not provide fixes for them.

Step 3: Check logs for signs of compromise

- The advisory says to look for unauthorised access, especially unexpected changes to or by the user 1 account. Confirm the user 1 email address is set to something you control.
- If signs of compromise are found, the advisory recommends reviewing guidance for hacked Drupal sites before making further changes.

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-2026-136716 in Drupal Core (CVSS 9.8), confirmed by the vendor as exploited in the wild. The flaw lets an unauthenticated attacker take over a Drupal site through the installer when the site is in an unusual or incomplete installation state. Please confirm: (1) whether we run Drupal Core and on which version; (2) whether install.php is publicly accessible; and (3) whether logs show unexpected changes to the user 1 account. Fixed versions are Drupal 10.6.23, 11.3.23, and 11.4.14; update.php must be run after upgrading. CISA's deadline is 30 November 2026. Please send written confirmation of the version, installer status, and patch status by 30 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:

- The advisory says to check for unexpected changes to or by the user 1 account in site logs.
- Check whether the user 1 email address has been changed to an address you do not control.
- Look for requests to install.php in the web server access log, particularly any that suggest an install flow was stepped through.

The weakness behind it

The record classes this as CWE-754 (Improper Check for Unusual or Exceptional Conditions).

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 reachable over a network with no authentication via a public-facing installer file, which would likely be the initial entry point for a takeover.
Account Manipulation (T1098): Changing an existing account, for example adding permissions or keys, to keep access.	Persistence: staying in	The advisory says to check for unexpected changes to or by the user 1 account; site takeover would likely involve manipulating this privileged account.
Create Account (T1136): Creating a new account so the attacker can come back later.	Persistence: staying in	An installer under attacker control can create new administrative accounts; this would be a likely persistence mechanism following a site takeover.

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 an improper check for unusual or exceptional conditions vulnerability that allows an unauthenticated remote attacker to take over a site via the exposed Drupal installer when the site is in one of the affected unusual or incomplete installation states.*

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

> *Improper Check for Unusual or Exceptional Conditions vulnerability in Drupal Drupal core allows Forceful Browsing. This issue affects Drupal core versions: from 0.0.0 to 10.6.23, from 11.0.0 to 11.3.23, from 11.4.0 to 11.4.14.*

Versions of Drupal core the record lists as affected:

- 0.0.0 up to, but not including, 10.6.23
- 11.0.0 up to, but not including, 11.3.23
- 11.4.0 up to, but not including, 11.4.14

The affected ranges end before 10.6.23, 11.3.23, 11.4.14. 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-2026-136716
```

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-2026-136716
```

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 define exactly what unusual or incomplete install states look like or how to identify them other than through log review.
- The sources do not say whether Drupal Steward covers all possible attack vectors or only those known at the time of the advisory.
- The sources do not state when exploitation began or how widely it is occurring.
- We have not tested this against any environment. Versions and scores are as the sources state them and as at 27 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. Severity decoded

CVE-2026-136716: score 9.8, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H` As the CVE record gives it. The record's own score can differ from the base score on the NVD record.

Metric	Value	What it means here
Attack vector	Network	Reachable over a network, with no need to be on the same segment.
Attack complexity	Low	No special conditions beyond the flaw itself.
Privileges required	None	No account is needed.
User interaction	None	No one has to do anything.
Scope	Unchanged	Damage stays inside the vulnerable component.
Confidentiality	High	Total loss of confidentiality.
Integrity	High	Total loss of integrity.
Availability	High	Total loss of availability.

Appendix 2. Timeline

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

Appendix 3. 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 installer reachable and signs of unexpected changes to user 1	High	Immediately; treat as likely compromised
Drupal site on an affected version with installer reachable, no known signs of compromise	High	Before 30 November 2026
Drupal site on an affected version; installer accessibility unknown	High	Before 30 November 2026; confirm installer status first

Drupal site on an affected version with installer already secured	Medium	Patch at next planned maintenance window
Drupal site already on a fixed version (10.6.23, 11.3.23, or 11.4.14)	Low	Confirm update.php has been run

Appendix 4. 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-2026-136716: https://www.cve.org/CVERecord?id=CVE-2026-136716
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Advisory or release notes read: www.drupal.org/sa-core-2026-019: https://www.drupal.org/sa-core-2026-019