contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Vanderbilt University Research Electronic Data Capture (REDCap) exploited

CVE-2026-90817 · on CISA's exploited list since 18 November 2026

Analysis Report

If you run REDCap 13.3.0 or later, upgrade to 16.0.49, 17.3.10 or 17.4.4 by 21 November 2026. First find out whether and where you run it. If you do not run

PREPARED BY	NamiQ	DATE	18 November 2026
FACTS AS OF	18 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 3.1 9.8**	STATUS	On CISA's exploited list; due 21 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/vanderbilt-university-research-electronic-cve-2026-90817

The bottom line

> *If you run REDCap 13.3.0 or later, upgrade to 16.0.49, 17.3.10 or 17.4.4 by 21 November 2026. First find out whether and where you run it. If you do not run REDCap, you can stop reading.*

At a glance

Fact	Detail
Product	Vanderbilt University Research Electronic Data Capture (REDCap) (CVE-2026-90817)
Severity	Critical: 9.8 (CVSS 3.1)
CISA	On its exploited list since 18 November 2026. Deadline for US federal agencies: 21 November 2026.
Chance of exploitation (EPSS)	0.04, the estimated chance in the next 30 days, as at 18 November 2026
Ransomware use	Not recorded by CISA. That is not the same as none.
Fixed in	REDCap 16.0.49 LTS, 17.3.10 LTS or 17.4.4 Standard Release, as applicable (CVE record; no fix date given)
Who looks first	Whoever runs a REDCap server on 13.3.0 or later, especially one that hosts public surveys. The attacker needs a valid public survey hash.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run REDCap, or does a supplier run it for you?	Nothing to do for this CVE.	Find the version (next question).
Is the version 13.3.0 or later?	The record does not list you as affected; confirm the version in writing.	You are in the affected range. Go to the next question.
Does the server host public surveys that can be reached from the internet?	The attack needs a public survey hash, so exposure is lower. Still patch.	Treat as urgent. Patch within CISA's window.
Are you already on 16.0.49, 17.3.10 or 17.4.4 (or a later release)?	Upgrade to the release line you follow.	The record names these as unaffected. Keep the evidence.

What it is

An attacker with no login can send crafted web requests that reach a route not meant for a public survey. They then pass a crafted file path during data import. The record says this lets them run code on the REDCap server.

Why it matters

Our reading: this is code execution on a server, started from outside, with one precondition. The attacker needs a valid public survey hash, and public surveys exist to be shared, so that condition may be easy to meet. A REDCap server holds the data it was given, so a foothold would be useful for reading or changing that data and as a base inside the network. The score is 9.8 on CVSS 3.1. The weaknesses are CWE-73 (file name or path control) and CWE-94 (code generation control).

Things people will get wrong

- "The attacker must be logged in." The record and CISA both say no authentication is needed. What the attacker needs is a valid public survey hash.
- "We have no public surveys, so this does not apply." The record lists REDCap 13.3.0 and higher as affected. Having no public surveys may reduce exposure, but the sources do not say it removes the flaw.
- "Any recent version is fixed." The record names only three unaffected releases: 16.0.49, 17.3.10 and 17.4.4. Check your exact version against them.

The wording includes conditions the score may not show: the attacker must be logged in. Read the record before you decide it does not apply to you.

How we would triage it

This is our judgement.

Step 1: Find the REDCap versions you run

- Ask whoever administers REDCap for the exact version. The record says 13.3.0 and higher is affected.
- Include test, training and supplier-hosted copies. They are easy to forget.

Step 2: Reduce exposure while you wait

- List which public surveys are live and close any that are not needed.
- The sources name no workaround. Do not assume that hiding a survey link fixes the flaw.

Step 3: Upgrade to a fixed release

- Move to 16.0.49 LTS, 17.3.10 LTS or 17.4.4 Standard Release, whichever matches the line you follow.
- CISA's required action is to apply the vendor's mitigations. Take a backup first.

Step 4: Check the result

- Confirm the running version is one of the three named releases.
- Review web and application logs from before the upgrade for the signs listed on this page.

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.

> *Hello, we need to confirm our exposure to CVE-2026-90817, a flaw in Vanderbilt University REDCap. The CVE record says an unauthenticated attacker may be able to run code on the server. It affects REDCap 13.3.0 and higher. Please tell us whether we run REDCap, where, and which version. The record names 16.0.49, 17.3.10 and 17.4.4 as unaffected. CISA's deadline is 21 November 2026. Please confirm in writing, by that date, the version we run and that it is a fixed release, or when it will be upgraded. Thank you.*

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:

- Web requests to survey pages that carry an unusual file path or stream value, or that reach a route not normally used by surveys.
- New or changed files in the REDCap web directory, or unexpected processes started by the web server account.
- Data import activity that no user can account for.

The weakness behind it

The record classes this as CWE-94 (Improper Control of Generation of Code) and CWE-73 (External Control of File Name or Path).

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 reached through crafted HTTP requests from a public survey with no login, so exploitation would likely start at an internet-facing web application.
Command and Scripting Interpreter (T1059): Running commands or scripts on a machine, such as a shell or PowerShell.	Execution: running the attacker's code	The record says an attacker could execute arbitrary code on the server. A successful exploit would typically give a way to run commands there.

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:

> *Vanderbilt University Research Electronic Data Capture (REDCap) contains a code injection vulnerability which could allow an unauthenticated attacker to execute arbitrary code on the server. An attacker could exploit this via crafted HTTP requests that access an unintended controller route from a public survey context and supply a crafted file-path or stream parameter during data import processing. Exploitation requires knowledge of a valid public survey hash.*

The CVE record, published by Securifera on 20 September 2026:

> *An unauthenticated Remote Code Execution vulnerability was found in the survey passthrough routing and Data Import processing logic, in which a malicious user could potentially exploit it by manipulating HTTP requests to access an unintended controller route from a public survey context and by supplying a crafted file-path/stream parameter during import handling. If successfully exploited, this could allow the attacker to remotely execute arbitrary code on the REDCap server. The attacker does not have to be authenticated in order to exploit this, but exploitation requires knowledge of a valid public survey hash. This vulnerability exists in REDCap 13.3.0 and higher.*

Versions of Vanderbilt University REDCap the record lists as affected:

- 13.3.0

It lists these as unaffected:

- 16.0.49
- 17.3.10
- 17.4.4

What the record says to do about it, in the vendor's words:

> *Upgrade to REDCap 16.0.49 LTS, 17.3.10 LTS, or 17.4.4 Standard Release, as applicable.*

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-2026-90817
```

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-2026-90817
```

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

- Whether any workaround exists. The CVE record names only upgrading.
- Whether releases other than 16.0.49, 17.3.10 and 17.4.4 are fixed; the sources do not say.
- How an attacker would normally obtain a public survey hash; the sources do not say.
- Which earlier releases, if any, were affected before 13.3.0; the record lists none.
- We have not tested this against any environment. Versions and scores are as the sources state them and as at 18 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-2026-90817: 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
20 September 2026	CVE record published by Securifera.
18 November 2026	CISA added it to its list of exploited vulnerabilities.
21 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
REDCap 13.3.0 or later with public surveys reachable from the internet	High	within CISA's window
REDCap 13.3.0 or later, reachable only from an internal network	Medium	this week
REDCap run by a supplier or host on your behalf, version unknown	Medium	ask now; confirmation within CISA's window

REDCap already on 16.0.49, 17.3.10 or 17.4.4	Low	keep the confirmation; no action
No REDCap anywhere in your estate	None	none for this CVE

Appendix 4. Definition of done

- Every Vanderbilt University Research Electronic Data Capture (REDCap) 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-2026-90817: https://www.cve.org/CVERecord?id=CVE-2026-90817
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Advisory or release notes read: projectredcap.org/resources/community/: https://projectredcap.org/resources/community/
- Reference in the CVE record: www.securifera.com: https://www.securifera.com/advisories/