contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

PrefectHQ prefab-ui: new CVE

CVE-2026-120338 · record published 1 November 2026

Analysis Report

Only relevant if you run PrefectHQ prefab-ui. Any installation on 0.14.0 through 0.20.x with the GenerativeUI sandbox reachable carries a score-10 flaw; no CISA deadline has been set. Start by …

PREPARED BY	NamiQ	DATE	2 November 2026
FACTS AS OF	2 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 3.1 10.0**	STATUS	Not on CISA's exploited list; exploitation not recorded

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/prefecthq-prefab-ui-cve-2026-120338

The bottom line

> *Only relevant if you run PrefectHQ prefab-ui. Any installation on 0.14.0 through 0.20.x with the GenerativeUI sandbox reachable carries a score-10 flaw; no CISA deadline has been set. Start by confirming the installed version and whether FastMCP's GenerativeUI tool is exposed.*

At a glance

Fact	Detail
Product	PrefectHQ prefab-ui (CVE-2026-120338)
Severity	Critical: 10 (CVSS 3.1)
Status	A new CVE record, published by JFROG on 1 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 2 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	prefab-ui 0.21.0 is the first unaffected version per the record (affected range: 0.14.0 before 0.21.0). PyPI shows 0.21.1 as the latest available release.
Who looks first	Teams running prefab-ui through FastMCP with the GenerativeUI provider in use, where any caller — a user, an agent, or another service — can submit code to the generate_prefab_ui MCP tool.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run PrefectHQ prefab-ui in any service, container, or Python environment?	Nothing to do for this CVE.	Check the installed version (next question).
Is the installed version between 0.14.0 and 0.20.x (before 0.21.0)?	You are not on an affected version.	Check whether GenerativeUI is in use (next question).
Is the FastMCP GenerativeUI provider, or any path that calls the GenerativeUI sandbox, enabled?	Lower priority; upgrade to 0.21.0 at the next patch cycle.	Any caller who can reach generate_prefab_ui can exploit this; continue.
Can a caller outside your organisation, or without authentication, reach that tool?	Upgrade urgently; restrict the tool's exposure in the meantime.	Treat as actively exploitable; upgrade immediately and check for persistence.

What it is

The sandboxed Python environment meant to isolate untrusted or LLM-written code does not actually isolate it: caller-supplied Python can read and write any file the server process can reach, and can persist itself by writing into the server's Python environment.

Why it matters

Our reading is that the score of 10 reflects three weaknesses together: the sandbox's advertised protection (CWE-693) is absent, caller-supplied code runs with server-level file access (CWE-94), and the Deno subprocess has unrestricted read, write, and network permissions (CWE-269). The persistence mechanism the record describes — writing into site-packages — survives a service restart. The typical entry point, the FastMCP generate_prefab_ui tool, may require no authentication, depending on how the server is deployed.

Things people will get wrong

- "The sandbox at least blocks outbound network calls." The record says the Deno subprocess is granted unrestricted read, write, and network permissions, so outbound network access is also unrestricted.
- "Only AI-generated UIs are at risk; hand-authored code is safe." The record says any caller who can supply the code argument to the sandbox is affected; the flaw is in the launcher's permissions, not in how the code was written.

How we would triage it

This is our judgement.

The commands only read: they print a version or list what is installed. They come from general knowledge of this kind of product, not from the sources, so check them against the vendor's page before you run them. Words in capitals are for you to fill in.

Step 1: Find the installed prefab-ui version

- Check every Python environment — virtualenvs, containers, and CI runners — where prefab-ui may be installed.
- The affected range is 0.14.0 through 0.20.x (before 0.21.0); the record does not list versions before 0.14.0 as affected.

```
pip show prefab-ui
pip list | grep prefab
```

Step 2: Confirm whether the GenerativeUI sandbox is in use

- Look for any service that imports FastMCP's GenerativeUI provider or that forwards caller code to prefab-ui's sandbox.
- If the generate_prefab_ui MCP tool is registered and reachable by callers, the exploitation path exists.

Step 3: Upgrade to prefab-ui 0.21.0 or later

- The record states 0.21.0 is the first unaffected version; PyPI shows 0.21.1 is available.
- Restart any running service after upgrading — a restart without a package update does not change the code in use.

Step 4: Check for persistence if the service was exposed

- The record identifies files written to the server virtualenv's site-packages as the persistence mechanism; look for unexpected entries there.
- Also check for files with recent modification times in any directory the application process can write to.

```
pip show prefab-ui | grep Location
```

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.

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 reviewing CVE-2026-120338, a score-10 flaw in PrefectHQ prefab-ui versions 0.14.0 through 0.20.x. The flaw allows a caller who can submit code to the GenerativeUI sandbox to read and write files on the server and write a persistence mechanism into the Python environment. The first unaffected version is 0.21.0. Please confirm whether prefab-ui is installed anywhere in our systems, which version is running, whether the FastMCP GenerativeUI feature is enabled and who can reach it, and when it can be upgraded to 0.21.0 or later. Please reply in writing with confirmation of the version and the fix plan by 9 November 2026.*

The weakness behind it

The record classes this as CWE-693 and CWE-94 and CWE-269.

The sources, in their words

The CVE record:

> *Prefab UI's Generative UI sandbox runs caller-supplied Python inside Pyodide, Python compiled to WebAssembly, in a Deno subprocess. The feature is documented as isolation for untrusted code, including LLM-written UI. From prefab-ui 0.14.0 through 0.20.2 the launcher starts Deno with unrestricted --allow-read, --allow-write, and --allow-net, and the runner leaves the Deno API on the JavaScript global object. Pyodide's js module proxies that global, so the Python can call Deno.readTextFileSync and Deno.writeTextFileSync. A caller who can supply the code can read and write files as the server OS user, and can persist code execution by writing a .pth file into the server virtualenv's ...*

Versions of PrefectHQ prefab-ui the record lists as affected:

- 0.14.0 up to, but not including, 0.21.0

What we do not know yet

- Whether removing the FastMCP GenerativeUI provider, without upgrading, is a fully effective workaround.
- Whether the fix in 0.21.0 restricts all three permissions (read, write, and network) or only some of them.
- Whether versions before 0.14.0 are unaffected because the GenerativeUI feature was not yet present, or for another reason.
- Exploitation is not recorded. That is not the same as none.
- This is a new record: scores, versions and wording can change in the first days, and they are as at 2 November 2026. We read the vendor pages listed under Sources; nothing here has been tested.
- 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", "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-2026-120338: score 10, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H` As the CVE record gives it.

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	Changed	Damage reaches beyond 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
1 November 2026	CVE record published by JFROG.

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
Affected version, GenerativeUI tool reachable over the network without authentication	Medium	Upgrade now; this week at the latest
Affected version, GenerativeUI enabled but only authenticated callers can reach it	Medium	Upgrade this week
Affected version installed but GenerativeUI not in use	Low	Upgrade at next patch cycle
prefab-ui 0.21.0 or later installed	None	None for this CVE

Appendix 4. Definition of done

- Every PrefectHQ prefab-ui you run is listed, with its version.
- Each is outside the affected list, or the vendor's fix or mitigation is in place.
- The version output or a screenshot is saved with the date.
- Anything not done has an owner and a date.

Sources

- CVE record for CVE-2026-120338: https://www.cve.org/CVERecord?id=CVE-2026-120338
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Advisory or release notes read: github.com/PrefectHQ/prefab: https://github.com/PrefectHQ/prefab
- Advisory or release notes read: pypi.org/project/prefab-ui/: https://pypi.org/project/prefab-ui/
- Reference in the CVE record: github.com: https://github.com/PrefectHQ/prefab/security/advisories/GHSA-595q-jv4r-q7j9
- Reference in the CVE record: github.com: https://github.com/PrefectHQ/prefab/pull/538
- Reference in the CVE record: github.com: https://github.com/PrefectHQ/prefab/commit/030f074f85e0b1be0dd44b0283185aecb26337a2