contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

xianhc ape-volo-admin: new CVE

CVE-2026-120442 · record published 2 November 2026

Analysis Report

Any team running ape-volo-admin before 3.6.1 should update this week: the record scores this 9.8 and no login is needed to exploit it. Update to 3.6.1, released 31 October 2026; if you do not run …

PREPARED BY	NamiQ	DATE	3 November 2026
FACTS AS OF	3 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 3.1 9.8**	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/xianhc-ape-volo-admin-cve-2026-120442

The bottom line

> *Any team running ape-volo-admin before 3.6.1 should update this week: the record scores this 9.8 and no login is needed to exploit it. Update to 3.6.1, released 31 October 2026; if you do not run this software, you can stop reading.*

At a glance

Fact	Detail
Product	xianhc ape-volo-admin (CVE-2026-120442)
Severity	Critical: 9.8 (CVSS 3.1)
Status	A new CVE record, published by VulnCheck on 2 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 3 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	3.6.1, released 31 October 2026
Who looks first	Teams that self-host xianhc ape-volo-admin, any version before 3.6.1. The flaw is in the application itself, present regardless of whether the admin interface faces the internet.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run xianhc ape-volo-admin?	Nothing to do for this CVE.	Check which version is installed.
Is the installed version earlier than 3.6.1?	You are on the fixed version. Nothing further to do.	Vulnerable; update to 3.6.1. Review release notes first — breaking changes apply.
Can untrusted users or hosts reach the admin API?	Risk is lower; update at your next patch cycle.	Update this week; exposure is live.

What it is

An attacker can forge a valid administrator token entirely offline, without ever connecting to the system, by using a signing key that the record says is hardcoded in the application's configuration file. With that token they gain full API control over users, roles, permissions and data.

Why it matters

CWE-1394 (use of a hardcoded cryptographic key) means the attack requires no network position and no brute force: anyone who can read the source can sign a token. The score of 9.8 reflects that no authentication whatsoever is needed. Our reading is that the risk is not limited to internet-facing deployments — any insider or compromised host that can reach the API at all can escalate to full administrator access once the key is known, and the key is fixed in code.

What the vendor's advisory says

We read two pages on github.com. In short:

- The GitHub release notes for V3.6.1, dated 31 October 2026, describe a major refactoring of the application and an upgrade to .NET 10, merging the front and back-end source trees into a single repository.
- The release notes include a BREAKING CHANGE notice: project paths, API routes and configuration structure have all changed, and existing deployments and callers must adapt before upgrading.
- The release notes state that the release also addresses security issues in role assignment, menu links, rate limiting and monitoring access, though no separate CVE identifiers are given for those items.

Things people will get wrong

- Attackers need network access to the running system to exploit this. The record says tokens can be forged entirely offline. An attacker needs only the hardcoded signing key and the administrator account ID, both obtainable without touching the live system.
- Blocking the admin API from the internet removes the risk. Restricting external access reduces exposure but does not remove the flaw. Any insider or compromised internal host that can reach the API can still present a forged token. The fix is updating to 3.6.1.

How we would triage it

This is our judgement.

Step 1: Find the version installed

- Check the application's startup log, deployment manifest, or about endpoint for the version string.
- If deployed from source, check the git tag or the project file for the version number.

Step 2: Restrict access while you prepare the update

- If the admin API is reachable from outside your trusted network, block it at the firewall or reverse proxy until the update is applied.
- The record says the flaw gives full API control over users, roles, permissions and data; treat any untrusted access path as live exposure until patched.

Step 3: Update to 3.6.1

- The vendor's release notes for V3.6.1 flag a BREAKING CHANGE: project paths, API routes and configuration structure have changed. Review the release notes before deploying.
- Update to 3.6.1, released 31 October 2026, which the vendor confirmed on 2 November 2026 resolves this vulnerability.

Step 4: Verify the update

- Confirm the running version is 3.6.1 after deployment.
- Review admin API logs for any unexpected calls to user, role or permission endpoints, particularly from unfamiliar addresses or outside normal working hours.

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 writing regarding CVE-2026-120442, a 9.8-severity authentication bypass in xianhc ape-volo-admin affecting all versions before 3.6.1. The record states that an attacker can forge administrator tokens offline using a hardcoded signing key, giving full API access to users, roles, permissions and data without any login. Could you confirm whether we run this application, which version is installed, and whether it has been updated to 3.6.1, released 31 October 2026? Please send us written confirmation of the version in use and the status of the fix by 10 November 2026.*

The weakness behind it

The record classes this as CWE-1394.

The sources, in their words

The CVE record:

> *ape-volo-admin before 3.6.1 contains an authentication bypass vulnerability that allows unauthenticated attackers to forge administrator tokens using a hardcoded JWT signing key in appsettings.json. Attackers can sign tokens offline with the jti claim set to the seeded administrator id to gain full API control over users, roles, permissions and data.*

Versions of xianhc ape-volo-admin the record lists as affected:

- all versions up to, but not including, 3.6.1

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-2026-120442
```

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 names of running container images 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-2026-120442
```

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. It reads the names of the running images, not what is 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 sources do not say whether the hardcoded signing key is the same value across all installations or differs per deployment.
- The sources do not say whether administrator tokens forged before the fix remain valid after upgrading to 3.6.1, or whether existing sessions must be explicitly revoked.
- The sources do not give CVE identifiers for the other security issues addressed in the V3.6.1 release alongside this one.
- The sources do not say when the hardcoded key was introduced, so it is unclear whether versions earlier than 3.5.2 are also affected.
- 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 3 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-2026-120442: 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.

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
2 November 2026	CVE record published by VulnCheck.

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
ape-volo-admin before 3.6.1 with the admin API reachable from the internet	High	This week
ape-volo-admin before 3.6.1 on an internal network reachable by untrusted users or hosts	High	This week
ape-volo-admin before 3.6.1 on a network accessible only to trusted administrators	Medium	Next patch cycle
ape-volo-admin 3.6.1 already deployed	None	None for this CVE

Appendix 4. Definition of done

- Every xianhc ape-volo-admin 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-2026-120442: https://www.cve.org/CVERecord?id=CVE-2026-120442
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Advisory or release notes read: github.com/xianhc/ape-volo-admin/releases/tag/V3.6.1: https://github.com/xianhc/ape-volo-admin/releases/tag/V3.6.1
- Advisory or release notes read: github.com/xianhc/ape-volo-admin/issues/36: https://github.com/xianhc/ape-volo-admin/issues/36
- Reference in the CVE record: github.com: https://github.com/xianhc/ape-volo-admin/commit/938f7ec58047f0c63123dc155d6a033910f00933
- Reference in the CVE record: github.com: https://github.com/xianhc/ape-volo-admin/blob/V3.5.2/Ape.Volo.Api/appsettings.json#L4-L10
- Reference in the CVE record: github.com: https://github.com/xianhc/ape-volo-admin/blob/V3.5.2/Ape.Volo.Infrastructure/Extensions/AuthorizationExtensions.cs#L50-L60