contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

UnrealIRCd exploited

CVE-2026-114713 · on CISA's exploited list since 13 November 2026

Analysis Report

If you run UnrealIRCd with two or more linked servers, act now: CISA's date of 16 November 2026 has passed. Apply the vendor's hot-patch or upgrade to 6.2.7.1 first. If you run no IRC server, or only …

PREPARED BY	NamiQ	DATE	18 November 2026
FACTS AS OF	18 November 2026	VERSION	1.0
SEVERITY	**High: CVSS 3.1 8.6**	STATUS	On CISA's exploited list; due 16 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/unrealircd-cve-2026-114713

The bottom line

> *If you run UnrealIRCd with two or more linked servers, act now: CISA's date of 16 November 2026 has passed. Apply the vendor's hot-patch or upgrade to 6.2.7.1 first. If you run no IRC server, or only a single unlinked one, you can stop reading.*

At a glance

Fact	Detail
Product	UnrealIRCd (CVE-2026-114713)
Severity	High: 8.6 (CVSS 3.1)
CISA	On its exploited list since 13 November 2026. Deadline for US federal agencies: 16 November 2026.
Chance of exploitation (EPSS)	0.00, 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	UnrealIRCd 6.2.7.1 (vendor release, 7 November 2026), or the vendor's hot-patch bundle-20261107 that needs no restart.
Who looks first	Anyone who runs an UnrealIRCd server, or has an IT provider who does, on a version before 6.2.7.1, especially a network of two or more linked servers that ordinary users can connect to.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run UnrealIRCd, or does a provider run it for you?	Nothing to do for this CVE.	Check the version (next question).
Is the version before 6.2.7.1?	You already have the fix. Ask for written confirmation.	Go on to the next question.
Does the network link two or more servers?	The record describes linked servers only. Still patch, but with less urgency.	Patch now: hot-patch or upgrade.
Can ordinary users, or anyone on the internet, connect to it?	Exposure is lower. Patch in your next window and keep access limited.	Treat as exposed. Patch first, then check the logs.

What it is

The record says the labeled-response module copies a message tag into replies without escaping it. Any user on a network with two or more linked servers can use this to inject server-to-server commands. Those commands run with server authority.

Why it matters

The vendor's own news item calls this the critical one of nine security issues fixed in 6.2.7.1, and says it lets normal users run commands with server or IRCOp authority. Our reading is that this turns an ordinary chat account into control of the network, so a low-privilege user is enough. The vendor says almost all version 6 networks can hot-patch without a restart, which removes the usual reason to delay.

What the vendor's advisory says

We read two pages on www.unrealircd.org. In short:

- The vendor's news item says 6.2.7.1 and a hot-patch were released on 7 November 2026 to fix 9 security issues, one rated critical.
- The vendor says the critical issue lets normal users execute commands with server or IRCOp authority.
- The vendor says that on almost all version 6 networks all these issues can be hot-patched without a restart.
- The vendor's earlier notice of 4 November 2026 recommended running a hot-patch test beforehand.

Things people will get wrong

- "It needs an admin account to exploit." The record says any user on a network with two or more linked servers can do it. No operator rights are mentioned.
- "We would have to restart the IRC server to patch." The vendor says almost all version 6 networks can use the hot-patch without a restart. Check that yours is one.
- "We are patched because we run 6.2.7." The record says versions before 6.2.7.1 are affected, so 6.2.7 is in range.

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 versions you run

- Ask who runs UnrealIRCd, and on which servers. The record covers all versions before 6.2.7.1.
- Note whether servers are linked, because the record describes that setup.

```
ps -ef | grep -i [u]nrealircd
```

Step 2: Reduce exposure

- Until patched, limit who can connect to linked servers where you can. The sources name no other workaround.

Step 3: Patch

- Apply the vendor's hot-patch bundle-20261107, or upgrade to 6.2.7.1 or later.
- The vendor says the hot-patch fixes the issue without a restart.

Step 4: Check and record

- Confirm the running version and that the patch loaded.
- Review logs for the period before patching, then keep written confirmation.

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 know whether we run UnrealIRCd, on which servers, and which version, in connection with CVE-2026-114713. The record says versions before 6.2.7.1 are affected. The vendor's fix is 6.2.7.1, or the hot-patch bundle-20261107 that needs no restart. CISA's date for this was 16 November 2026. Please confirm in writing the version we run and that the fix is in place, by the end of this week. 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:

- Server-to-server commands or unusual server notices that arrived from a normal user connection.
- Messages containing a label tag with line-break or delimiter characters.
- Unexpected changes made by server authority, such as new bans, operator rights or links.

The weakness behind it

The record classes this as CWE-140 (Improper Neutralization of Delimiters).

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 record says any user on a linked network can reach it, so a public-facing chat service would likely be the way in.
Command and Scripting Interpreter (T1059): Running commands or scripts on a machine, such as a shell or PowerShell.	Execution: running the attacker's code	Injected server-to-server commands run with server authority, so this would typically let the attacker issue commands the server itself trusts.

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:

> *UnrealIRCd UnrealIRCd contains an improper neutralization of delimiters vulnerability that allows any user on a network with two or more linked servers to inject server-to-server commands that are executed with server authority.*

The CVE record, published by Mitre on 8 November 2026:

> *The labeled-response module in UnrealIRCd 6.0.0 before 6.2.7.1 does not escape the IRCv3 "label" message tag when echoing it into replies, which allows any user on a network with two or more linked servers to inject server-to-server commands that are executed with server authority.*

Versions of UnrealIRCd the record lists as affected:

- all versions before 6.2.7.1

The affected ranges end before 6.2.7.1. Those are the first versions the record does not list as affected; confirm them in the vendor's advisory.

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

> *Upgrade to UnrealIRCd 6.2.7.1 or later. Alternatively, apply the hot-patch to fix the issue without restart: ./unrealircd hot-patch bundle-20261107*

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-2026-114713
```

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-2026-114713
```

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 the flaw is exploitable on a single server with no links; the record describes linked servers only.
- Whether attackers have used it against particular networks; CISA lists it as exploited but gives no detail.
- Whether any workaround exists short of patching; the sources name none.
- How to tell from logs that it was used; the sources do not say.
- 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-2026-114713: score 8.6, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:H/A:N` 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	Changed	Damage reaches beyond the vulnerable component.
Confidentiality	None	No data exposed.
Integrity	High	Total loss of integrity.
Availability	None	No effect on availability.

Appendix 2. Timeline

Date	Event
8 November 2026	CVE record published by Mitre.
13 November 2026	CISA added it to its list of exploited vulnerabilities.
16 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
Linked servers on a version before 6.2.7.1, open to ordinary users	High	Now; CISA's date has passed
A single server, not linked, on a version before 6.2.7.1	Medium	This week; the record names linked servers
Version before 6.2.7.1 reachable only by trusted staff	Medium	This week

Already on 6.2.7.1 or later, or hot-patched	Low	Confirm in writing
You do not run UnrealIRCd	None	None for this CVE

Appendix 4. Definition of done

- Every UnrealIRCd 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-2026-114713: https://www.cve.org/CVERecord?id=CVE-2026-114713
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Advisory or release notes read: www.unrealircd.org: https://www.unrealircd.org/
- Advisory or release notes read: www.unrealircd.org/index/news: https://www.unrealircd.org/index/news
- Reference in the CVE record: forums.unrealircd.org: https://forums.unrealircd.org/viewtopic.php?t=9487