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 below 6.2.7.1, patch now; CISA sets 16 November 2026. Upgrade to 6.2.7.1 or apply the vendor's hot-patch, which the vendor says needs no restart. Networks linking two or more …

PREPARED BY	NamiQ	DATE	14 November 2026
FACTS AS OF	14 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 below 6.2.7.1, patch now; CISA sets 16 November 2026. Upgrade to 6.2.7.1 or apply the vendor's hot-patch, which the vendor says needs no restart. Networks linking two or more servers are most at risk.*

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)	0.01, the estimated chance in the next 30 days, as at 14 November 2026
Ransomware use	Not recorded by CISA. That is not the same as none.
Fixed in	UnrealIRCd 6.2.7.1 (released 7 November 2026); or the vendor's hot-patch bundle, which the vendor says fixes it without a restart.
Who looks first	Anyone running UnrealIRCd below 6.2.7.1, especially IRC networks that link two or more servers. The vendor says normal users on such a network can end up acting with server or operator authority.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run UnrealIRCd on any host?	Nothing to do for this CVE.	Check the version (next question).
Is any instance on a version before 6.2.7.1?	You are already on a fixed build.	It needs the fix (next question).
Does it link to one or more other servers?	Lower risk, but still patch.	Highest risk; patch now.

What it is

An ordinary logged-in user can smuggle server-to-server commands into the system by abusing an unescaped message tag, and those commands then run with server authority. The record says this works on any network that links two or more servers together.

Why it matters

This turns an ordinary user into something with server authority. On a linked network that is a full privilege jump, not just a crash or a leak. The vendor rates it critical and shipped a hot-patch it says needs no restart, which signals they want it fixed fast. Our reading is that any network linking two or more servers and letting users connect should treat this as urgent, because the only stated condition is being able to log in.

What the vendor's advisory says

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

- The vendor's news says 6.2.7.1, released 7 November 2026, fixes 9 security issues, of which one is rated critical — this one. The other eight are not detailed in these notes.
- The vendor says almost all UnrealIRCd 6 networks can apply the fix as a hot-patch without a restart, and recommended testing the hot-patch beforehand.

Things people will get wrong

- We only run one IRC server, so this cannot affect us. The record says the injection needs a network of two or more linked servers, so a lone server is lower risk; but patch anyway, since a server can be linked later.
- You would need an operator account to exploit this. The vendor says normal users can execute commands with server or operator authority, so no prior operator privilege is required.

How we would triage it

This is our judgement.

Step 1: Find the versions you run

- Check the running UnrealIRCd version against 6.2.7.1; the record says anything before it is affected.
- List every host that runs it, not just the main one, so none is missed.

Step 2: Check linking and exposure

- Note whether each server links to any others, since the record says the flaw needs two or more linked servers.
- Limit who can connect while you prepare the fix, as the stated condition is simply being a user on the network.

Step 3: Apply the fix

- Upgrade to 6.2.7.1, or apply the vendor's hot-patch, which the vendor says needs no restart.
- The vendor recommended running a hot-patch test beforehand.

Step 4: Confirm it is in place

- Re-check the version reads 6.2.7.1, or that the hot-patch has been applied, so the fix is proven rather than assumed.

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 would like to check our exposure to CVE-2026-114713 in UnrealIRCd. Could you confirm whether we run UnrealIRCd anywhere, on which hosts, and which version each runs? Anything before 6.2.7.1 is affected, and the fix is 6.2.7.1 or the vendor's no-restart hot-patch. CISA requires this fixed by 16 November 2026, and the flaw matters most where two or more servers are linked. Please apply the upgrade or hot-patch, and send us written confirmation of the version now running and that the fix is in place by 16 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:

- Server logs for unexpected server-to-server commands, or actions carrying server or operator authority that no operator initiated.

- Odd IRCv3 label message tags in client traffic, since the record says the flaw abuses an unescaped label tag echoed into replies.
- New or changed operator rights, bans or server links that you did not make around the exposure window.

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 describes a network-reachable IRC server where a connected user injects commands, so an attacker would likely reach it as an exposed network service to get in.
Exploitation for Privilege Escalation (T1068): Using a flaw to gain higher rights than the account had, such as administrator or root.	Privilege Escalation: gaining higher rights	The flaw lets a normal user act with server or operator authority, so an attacker with a plain account would likely use it to rise above their own privilege level.
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 weakness is unescaped input that injects server-to-server commands run with server authority, so an attacker would likely abuse it to issue commands they otherwise could not.

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

- The sources do not detail the other eight security issues fixed in 6.2.7.1, or how severe each is.
- The sources do not say which exact UnrealIRCd 6 sub-versions can take the hot-patch versus needing a full upgrade.
- The record does not describe how the flaw has been used in practice, only the weakness and the fix.
- We have not tested this against any environment. Versions and scores are as the sources state them and as at 14 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
UnrealIRCd below 6.2.7.1 running a network of two or more linked servers that users can connect to	High	within CISA's window
Public-facing UnrealIRCd below 6.2.7.1 where strangers can register and log in	High	within CISA's window
A single standalone UnrealIRCd server below 6.2.7.1 with no linked servers	Medium	this week

UnrealIRCd already on 6.2.7.1 or hot-patched	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