Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

UnrealIRCd Label-Tag Flaw Hands Server Authority to Ordinary Users

Date of Publication	Admiralty Code	TA Number
November 16, 2026	A1	TA2026338

Summary

First Seen: November 7, 2026
Affected Products: UnrealIRCd
Impact: CVE-2026-114713 lets any ordinary user on an UnrealIRCd network with two or more linked servers run commands with server or IRCOp authority, so a single crafted message can forcibly disconnect users with KILL, impose network-wide bans with GLINE, and carry out other privileged actions across the whole network. UnrealIRCd 6.0.0 through 6.2.7 and the end-of-life 5.x branch are affected. With exploitation confirmed by the vendor since November 8, 2026, a CISA KEV listing, and a working public exploit, unpatched networks face an immediate risk of mass disconnections, denial of service to legitimate users, and loss of trust in network administration. Servers on end-of-life releases are most exposed, because they receive no fixes.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-114713	UnrealIRCd Improper Neutralization of Delimiters Vulnerability	UnrealIRCd	✗	✓	✓

Vulnerability Details

#1

CVE-2026-114713 is a flaw in the labeled-response module of UnrealIRCd, which implements the IRCv3 "label" message tag that clients use to match replies to their requests. The module echoes the label back into replies without escaping it. Because the server first converts the IRCv3 escape `\n` in a tag value into a real line feed, and the 6.2.7 validator accepts any label of up to 64 bytes without checking its characters, an attacker can plant a line break inside the label. When the reply is built with raw formatting calls that skip the normal escaping routine and is routed over a server link, that line break splits it into two protocol lines.

#2

Exploitation needs only an ordinary client and a network with two or more linked servers. The public proof-of-concept sends one labeled two-parameter WHOIS, which forwards the query to a remote server and forces a labeled reply back across the link. The receiving server treats the injected second line, such as a KILL command, as coming from its trusted peer and runs it without the privilege checks applied to clients, even though the same KILL sent directly is refused with a 481 Permission Denied error. The same technique can set network-wide G-lines. A single server with no links is not exploitable, as the injected bytes are only echoed back to the attacker.

#3

UnrealIRCd 6.0.0 through 6.2.7 is affected, and so is the UnrealIRCd 5 branch, which reached end of life on July 1, 2023. The labeled-response module is on by default: the default modules.default.conf loads it, so most installs are exposed without any special setup. Versions 3.2.x and 4 were not checked, and the vendor believes several of the bugs fixed in this release go back as far as 3.2.x. The flaw is fixed in UnrealIRCd 6.2.7.1, which rejects any label containing a space, semicolon, backslash, carriage return or line feed. On most UnrealIRCd 6 networks, hot-patch bundle-20261107 applies the same fix without a restart. The release also fixes eight other security issues, including an IP address leak that lets a normal user decloak another user, a second IP address leak, and several crash, hang and denial-of-service conditions.

#4 In-the-wild exploitation is confirmed. The vendor updated its November 7, 2026 advisory to say attackers are exploiting the issue on the internet, and reported abuse attempts from November 8. CISA added the flaw to its Known Exploited Vulnerabilities catalog on November 13, 2026, with a remediation due date of November 16, 2026 and a forensic triage requirement under BOD 26-04.

#5 In proof-of-concept testing, successful exploitation left a trace in the test server's log: a `kill.KILL_COMMAND` entry whose "[by: ...]" field names a linked server instead of an operator, with leftover server protocol text such as "BATCH" and "labeled-response" in the kill reason. The PoC author took all captures against local lab instances, and neither the vendor nor CISA has published request patterns, victim counts or log signatures for this CVE.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-114713	UnrealIRCd UnrealIRCd (6.0.0 through 6.2.7; EOL 5.x also affected)	cpe:2.3:a:unrealircd:unrealircd:*:*:*:*:*:*:*:*	CWE-140

Recommendations

Migrate Off End-of-Life Releases: Plan the migration of every UnrealIRCd 3.2.x, 4 and 5 server to the supported 6.x branch. The vendor did not check 3.2.x and 4, believes several of the fixed bugs go back to 3.2.x, and warns that servers on end-of-life releases are not safe at all. Until migration is complete, add `blacklist-module "labeled-response";` to the configuration of every UnrealIRCd 5 server and perform a full restart, since a rehash is not enough.

Deploy the Spamfilter Workaround Immediately: The vendor asks admins to do this step before anything else. An IRCOp should run the following command once on the network, entered as a single line:

```
SPAMFILTER add -regex T block - Invalid_label ^label=(?![^\r\n;\x20]*\z)
```

It blocks any label that contains a carriage return, line feed, semicolon or space. This single command protects every linked server against the critical issue, but only if all servers run 6.0.4 or newer. It does not fix the other eight security issues, so it must be followed by the hot-patch or the upgrade.

Hot-Patch or Upgrade Every Server: On UnrealIRCd 6.0.0 through 6.2.7 on *NIX, run `./unrealircd hot-patch bundle-20261107` on every server; a successful run ends with "Patch installed and server rehashed correctly. All should be good now!" or, on older versions, "Done! All should be good now". On Windows, or if the hot-patch fails, upgrade to 6.2.7.1 by running `./unrealircd upgrade` on *NIX or downloading the release from the vendor's website, then restart the server. The vendor's "Hot-patching failed" FAQ covers common failures, such as a distribution upgrade breaking the build. Applying the hot-patch or the upgrade also fixes the eight other security issues in the release, including the decloaking and IP address leak flaws.

Verify Remediation on Each Node: On 6.0.2 or later, run `./unrealircd module-status | grep labeled-response` on every server. The output "labeled-response 5.0-hot-patch-bundle-20261107" or a version of 6.2.7.1 means the server is safe, while "5.0" without the patch bundle means the hot-patch was not applied. If there is no output, an IRCOp can check with `MODULE -all`, and can check remote servers with `MODULE -all` followed by the server name. Track the result for every leaf and hub. Optionally, once every server is patched, remove the temporary SPAMFILTER; this step comes from third-party guidance rather than the vendor.

Perform Forensic Triage: In line with CISA's BOD 26-04 forensic triage requirement, and given that the vendor has confirmed active exploitation since November 8, 2026, review server logs for `kill.KILL_COMMAND` and TKL entries whose "[by: ...]" field names a server rather than an operator account. A KILL issued by an ordinary user is always refused with a 481 Permission Denied error, so server-attributed kills that do not match services or administrative activity should be investigated. Leftover server protocol text such as "BATCH" and "labeled-response" in kill or ban reasons, and labeled replies whose label segment fails to parse on the receiving server, match what the proof-of-concept produced in lab testing. No log signatures from real attacks have been published, so treat these as leads to investigate rather than confirmed indicators.

Audit and Clean Up Network Bans: List all active G-lines and other network-wide bans and compare them against administrative records. Remove any unauthorized bans, notify affected users where appropriate, and reset any operator or services state that may have been changed through injected commands.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Privilege Escalation	T1068: Exploitation for Privilege Escalation	
Impact	T1531: Account Access Removal	
Impact	T1499: Endpoint Denial of Service	T1499.004: Application or System Exploitation

Patch Link

https://www.unrealircd.org/download/6.0

References

https://forums.unrealircd.org/viewtopic.php?t=9487

https://github.com/fixedbyreboot/CVE-2026-114713-POC

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

November 16, 2026 • 12:40 PM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com