GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

16 November 2026

Advisory 376: UnrealIRCd Improper Neutralization of Delimiters Vulnerability (CVE-2026-114713).

Release Date: 13th November 2026
Impact: HIGH
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above product(s). This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-114713 is a command injection vulnerability (CWE-140) in UnrealIRCd, a widely used open-source Internet Relay Chat (IRC) server. The labeled-response module does not escape the IRCv3 "label" message tag when it echoes the tag back in replies. On a network with two or more linked servers, any ordinary user can use this to insert server-to-server commands that the other servers carry out with server authority.

What are the systems affected?

The vulnerability affects UnrealIRCd servers that are linked to at least one other server:

- UnrealIRCd 6.0.0 through 6.2.7
- UnrealIRCd 5, which reached end of life on 1 July 2023 and will not receive a fix
- Single, unlinked servers are not exposed to this flaw but should still be updated, because 6.2.7.1 fixes eight other security issues

Not affected / patched version:

- UnrealIRCd 6.2.7.1 or later

- UnrealIRCd 6.0.0 to 6.2.7 with hot-patch bundle-20261107 applied

What does this mean?

Successful exploitation may allow attackers to:

- Run IRC operator and server commands as an ordinary user
- Disconnect (KILL) or ban (GLINE) users across the whole network
- Disrupt or take control of community, support or project chat channels
- Change network settings to keep control or hide their activity

Mitigation process

CERTVU recommends the following:

1. Apply the hot-patch or upgrade to 6.2.7.1
Apply hot-patch bundle-20261107 on every server running 6.0.0 to 6.2.7, following the UnrealIRCd project's instructions; it takes effect without a restart. Plan an upgrade to UnrealIRCd 6.2.7.1 from the official UnrealIRCd website, which also fixes eight other security issues, including IP address leaks and crash bugs.

2. Patch every linked server
The attack works across server links, so update all servers on the network, not only the one users connect to. Confirm that the labeled-response module on each server shows the patch bundle or version 6.2.7.1.

3. Apply the interim spamfilter rule if patching is delayed

4. Replace UnrealIRCd 5

5. Check for misuse
Review server logs for unexpected KILL, GLINE and other operator actions, unexplained changes to bans, channels or settings, and unusual label tags. No indicators of compromise have been published. Report suspected compromise to CERTVU at incident@cert.gov.vu.

Reference

1. https://forums.unrealircd.org/viewtopic.php?t=9487
2. https://www.cve.org/CVERecord?id=CVE-2026-114713
3. https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-114713
4. https://github.com/unrealircd/unrealircd/commit/05b5f5fdc8bb