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

27 August 2026

Advisory 199: CVE-2015-3246 - Red Hat Libuser Race Condition Vulnerability

Release Date: 26th August 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 products. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2015-3246 is a flaw in the way the libuser library handles the /etc/passwd file. The library modifies the file directly, so an authenticated local user who causes an error during that modification can leave the file in an inconsistent state, resulting in denial of service. Red Hat rated the issue as having Important security impact.
The vulnerability is significant principally because it can be chained. Combined with a related flaw, CVE-2015-3245, in which the userhelper program fails to filter newline characters supplied through its chfn interface, a local user can corrupt /etc/passwd in a controlled manner and escalate privileges to the root user. The two issues were discovered together by Qualys during an internal code audit and disclosed on 23 July 2015.

What are the systems affected?

The vulnerability affects the libuser library, used by the userhelper program in the usermode package.

libuser before version 0.56.13-8 - (Affected)
libuser 0.60 before version 0.60-7 - (Affected)
libuser 0.56.13-8, 0.60-7 and later - (Not affected, patched)

All versions of libuser included with Red Hat Enterprise Linux 6 and 7 were affected and have been addressed through vendor updates. Red Hat Enterprise Linux 5 was affected but was not planned to receive a fix, having already passed the relevant support phase.

What does this mean?

This is a local privilege escalation vulnerability, not a remote one. An attacker must already have the ability to run commands on the server before it can be used. That distinction is important for prioritisation, but it should not be read as reducing the seriousness of the issue.

Step 1 - Initial Foothold (separate vulnerability)
An attacker obtains the ability to execute commands on the server as an unprivileged user. In practice this most commonly follows the compromise of a public-facing web application, which yields a shell running as the web server account.

Step 2 - Reaching the Vulnerable Path
The attacker invokes the setuid-root userhelper program, which is available to any local user, and supplies crafted input through its interface for changing the user's own account details.

Step 3 - Corrupting /etc/passwd (CVE-2015-3246 with CVE-2015-3245)
Because newline characters are not properly filtered and libuser writes to /etc/passwd directly, the attacker introduces controlled content into the file.

Step 4 - Root Privileges
The manipulated account file yields root privileges, giving the attacker complete control of the server, its stored credentials, and any system that trusts it.

CERTVU emphasises the practical significance of this chain. A compromised web application ordinarily gives an attacker only the limited privileges of the web server account, which constrains what can be reached and how long access persists. A working local privilege

Mitigation process

CERTVU recommends the following:

1. **Update libuser and usermode Where a Vendor Update Is Available**

On supported Red Hat based distributions, apply the vendor update for libuser and usermode through the normal package manager.

2. **Rebuild Affected Container Images**

Rebuild any container images based on older Red Hat base images against current images, and redeploy. Updating the host does not update the libraries inside a container.

Other mitigation options include;

- Where No Vendor Update Exists, Remove the Setuid Privilege
- Migrate End-of-Life Systems
- Reduce the Value of a Foothold
- Review for Prior Compromise

Report suspected compromise to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. https://www.cve.org/CVERecord?id=CVE-2015-3246
2. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
3. https://access.redhat.com/articles/1537873
4. https://nvd.nist.gov/vuln/detail/CVE-2015-3246
5. https://www.cve.org/CVERecord?id=CVE-2015-3245