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 200: CVE-2015-5287 - Red Hat Automatic Bug Reporting Tool Privilege Escalation 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.

What is it?

CVE-2015-5287 is a link following vulnerability (CWE-59) in the abrt-hook-ccpp component of the Automatic Bug Reporting Tool, which writes core dump files to predictable filenames within its dump directories. Because those names are predictable and symbolic links are not handled correctly, a local user with write access to an ABRT problem directory can place a symbolic link in advance and cause the tool, running with elevated privileges, to write to a file of the attacker's choosing, allowing escalation to the root user.

The flaw was reported by Philip Pettersson of Samsung and fixed by Red Hat in RHSA-2015:2505, which also addressed the related issues CVE-2015-5273 and CVE-2015-5302. Red Hat rated the update as having Moderate security impact. Public exploit code and a module for a widely used penetration testing framework are both available.

What are the systems affected?

Automatic Bug Reporting Tool (ABRT) before version 2.7.1 - (Affected)

ABRT 2.7.1 and later, and Red Hat packages updated under RHSA-2015:2505 or later - (Not affected, patched)

On end-of-life distributions such as CentOS 7 no vendor update is available, and the mitigation guidance below applies.

What does this mean?

This is a local privilege escalation vulnerability. An attacker must already be able to run commands on the system before it can be used, so it is not an entry point in itself; its significance lies in what it enables afterwards.

An attacker who has compromised a public-facing application ordinarily holds only the limited privileges of the service account, which constrains what can be reached and how long access persists. A working escalation to root removes that constraint entirely, giving full control of the host, its stored credentials and any system that trusts it. Public exploit code and a ready-made framework module mean little skill is required to complete that step.

Servers providing shell accounts to staff, students or customers carry an additional exposure, as every account holder is already in a position to exploit the flaw without any prior compromise.

Mitigation process

CERTVU recommends the following:

1. **Determine Whether ABRT Is Installed and Active**

Check whether the package is present and whether ABRT is registered as the kernel crash handler. If the core pattern output references abrt-hook-ccpp, ABRT is active as the crash handler.

```
rpm -q abrt abrt-addon-ccpp
cat /proc/sys/kernel/core_pattern
```

2. **Apply the Vendor Update**

On supported distributions, update abrt and libreport through the normal package manager. This also addresses CVE-2015-5273 and CVE-2015-5302, which were fixed in the same advisory.

Other mitigation options include;

- Where No Update Is Available, Disable ABRT and Plan Migration
- 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-2015-5287
2. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
3. https://access.redhat.com/errata/RHSA-2015:2505
4. https://nvd.nist.gov/vuln/detail/CVE-2015-5287
5. https://cwe.mitre.org/data/definitions/59.html