

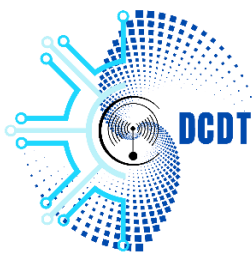
**GOVERNMENT OF THE REPUBLIC  
OF VANUATU**

PRIME MINISTER'S OFFICE

CERTVU  
DEPARTMENT OF COMMUNICATIONS  
& DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380



**GOVERNEMENT 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

9 October 2026

**Advisory 352: ISC BIND 9 TKEY Query Denial of Service Vulnerability -  
Actively Exploited (CVE-2015-5477).**

**Release Date:** 8th October 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-2015-5477 is a denial of service vulnerability (CWE-617, reachable assertion) in the TKEY query handling of ISC BIND 9, the most widely used DNS server software. A single crafted TKEY packet from an unauthenticated remote attacker triggers a REQUIRE assertion failure that makes the named daemon exit, taking DNS resolution offline. Both recursive and authoritative servers are affected, and access control lists or other configuration options do not prevent it, because the vulnerable code runs before those checks. A proof-of-concept exploit has been published, and Exploit-DB entries 37721 and 37723 exist. The CVSS v3.1 score is 7.5 (High) and the CVSS v2 score is 7.8.

## What are the systems affected?

The following ISC BIND 9 versions are affected:

- BIND 9.1.0 through 9.8.x (end of life, no fix issued)
- BIND 9.9.0 through 9.9.7-P1
- BIND 9.10.0 through 9.10.2-P2

Not affected / patched version:

- BIND 9.9.7-P2, 9.10.2-P3 or later. These branches are themselves long out of support, so upgrade to a currently supported BIND 9 release. Linux distributions have also published backported fixes (for example Red Hat RHSA-2015:1513 to 1515, Debian DSA-3319-1 and Ubuntu USN-2693-1)

## What does this mean?

Successful exploitation may allow attackers to:

- Crash the DNS service with one malicious packet, without credentials
- Cause an outage of name resolution for an organization, which disrupts websites, email and other services that depend on DNS
- Repeat the attack automatically, keeping a vulnerable server offline until the service is protected

## Mitigation process

CERTVU recommends the following:

### 1. Upgrade BIND

Upgrade to a currently supported BIND 9 release, or at minimum 9.9.7-P2 or 9.10.2-P3, and apply distribution security updates. No workaround exists, so patching is the remediation.

### 2. Find every BIND server

### 3. Reduce exposure

### 4. Plan for resilience

### 5. Monitor and report

Check logs for named assertion failures and repeated restarts, and report suspected attacks to CERTVU.

## Reference

1. <https://kb.isc.org/docs/aa-01272>
2. <https://nvd.nist.gov/vuln/detail/CVE-2015-5477>
3. <https://app.opencve.io/cve/CVE-2015-5477>
4. <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>