contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

ISC BIND exploited

CVE-2015-5477 · on CISA's exploited list since 8 October 2026

Analysis Report

If you run BIND as a DNS server, act now: CISA's deadline of 11 October 2026 has already passed. Check the version first. If you run no BIND, you can stop reading.

PREPARED BY	NamiQ	DATE	1 November 2026
FACTS AS OF	1 November 2026	VERSION	1.0
SEVERITY	**High: CVSS 3.1 7.5**	STATUS	On CISA's exploited list; due 11 October 2026

NamiQ © 2026 NamiQ. All rights reserved. This document is the property of NamiQ. It may be shared unaltered, with attribution.
Companion article: namiq.io/insights/isc-bind-cve-2015-5477

The bottom line

> *If you run BIND as a DNS server, act now: CISA's deadline of 11 October 2026 has already passed. Check the version first. If you run no BIND, you can stop reading.*

At a glance

Fact	Detail
Product	ISC BIND (CVE-2015-5477)
Severity	High: 7.5 (CVSS 3.1)
CISA	On its exploited list since 8 October 2026. Deadline for US federal agencies: 11 October 2026.
Chance of exploitation (EPSS)	1.00, the estimated chance in the next 30 days, as at 1 November 2026
Ransomware use	Not recorded by CISA. That is not the same as none.
Fixed in	No source we read names a fixed version
Who looks first	Anyone who runs ISC BIND as a DNS server, or whose IT provider does. Check name servers that answer queries from outside your network first.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you or your IT provider run ISC BIND (named) on any server or appliance?	Nothing to do for this CVE.	Find the version (next question).
Is the BIND version inside the affected range shown on this page?	Nothing further for this CVE. Keep a note of the version.	Treat it as affected and update.
Can anyone outside your organisation send queries to that server?	Lower urgency, but still update. Internal users could cause an outage.	Update first, and limit who can query it.
Is the server a vendor appliance or a packaged build?	Update BIND from your operating system or ISC.	Ask the vendor for their fixed build in writing.

What it is

A remote attacker can send specially crafted TKEY queries to the BIND name server (named). The record says this triggers an assertion failure and the daemon exits, so DNS stops answering until it is restarted.

Why it matters

The record gives a score of 7.5 and describes a denial of service only, not code execution or data theft. Our reading is that the use is taking down name resolution: when DNS stops, mail, web access and remote logins that depend on it fail too. Because CISA lists it as exploited, a name server that is reachable from the internet and not updated should be treated as a known target.

Things people will get wrong

- "It is only a denial of service, so it can wait." CISA lists it as exploited, and the record says the daemon exits. A stopped name server takes down everything that needs DNS.
- "The record is from 2015, so we must have patched it long ago." Age does not show a fix. Old servers and embedded builds can still be on affected versions, so check the version.
- "We would see an attack in our logs." The record does not say what a hit looks like. Do not rely on seeing it beforehand.

How we would triage it

This is our judgement.

The commands only read: they print a version or list what is installed. They come from general knowledge of this kind of product, not from the sources, so check them against the vendor's page before you run them. Words in capitals are for you to fill in.

Step 1: Find where BIND runs and which version

- Ask your IT provider for a list of DNS servers, including any inside routers or appliances.
- On each one, read the installed BIND version and compare it with the affected range on this page.

```
named -v
dpkg -l | grep -i bind9
```

Step 2: Reduce exposure while you plan the update

- Allow queries only from the networks that need them. The record does not name a workaround, so this is general hygiene, not a fix.
- Make sure a restart of the named service is quick, because the record says the daemon exits.

Step 3: Update to a fixed build

- No source here names a fixed version. Ask the vendor or your operating system supplier which build fixes CVE-2015-5477, and install it.
- Follow CISA's required action for the forensics step as well.

Step 4: Confirm the result

- Re-read the version on each server after the update.
- Ask for written confirmation that every BIND instance is on the fixed build.

To close it, read the version from the product itself, not from an old inventory, and save the output with the date. If you cannot update today, write down who owns it, the new date, and what limits exposure until then.

Send this to your IT provider

Copy it, change the names and dates, and send it. It is a draft for you to check, not a template tested with any provider.

> *Hello. CISA lists CVE-2015-5477, a denial-of-service flaw in ISC BIND (named) triggered by TKEY queries. Please tell us whether we run BIND anywhere, including inside routers or appliances, and which version each one is. Please also confirm which build fixes this CVE for each system, and whether any server answers queries from the internet. If any is affected, please update it and send us written confirmation of the new version by the end of this week. CISA's deadline of 11 October 2026 has already passed. Thank you.*

Signs it was used

An update closes the hole. It does not tell you whether someone used it first. CISA's required action points to its forensic triage requirements (BOD 26-04). Look for:

- Unexpected exits or restarts of the named service, particularly with an assertion message in its log.
- Gaps in DNS answers on the server at the times it stopped.

- Incoming TKEY queries from addresses you do not recognise, if your server logs query types.

The weakness behind it

CISA's entry classes this as CWE-19.

The sources, in their words

CISA's catalogue entry:

> *ISC BIND contains a data processing errors vulnerability that could allow remote attackers to cause a denial of service via TKEY queries.*

The CVE record, published by Mitre on 29 July 2015:

> *named in ISC BIND 9.x before 9.9.7-P2 and 9.10.x before 9.10.2-P3 allows remote attackers to cause a denial of service (REQUIRE assertion failure and daemon exit) via TKEY queries.*

The record gives no version ranges. Use the vendor's advisory for the affected versions.

CISA's required action:

> *Apply mitigations in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes).*

What we do not know yet

- Which BIND version is the first unaffected one: no vendor page could be read.
- Whether a workaround exists short of updating.
- What an attack looks like in logs or on the system.
- Whether embedded or vendor-packaged BIND builds are affected.
- We have not tested this against any environment. Versions and scores are as the sources state them and as at 1 November 2026; the vendor's advisory wins where it differs.
- The sections headed "The bottom line", "Does this apply to you?", "What it is", "Why it matters", "Exposure by situation", "Things people will get wrong", "How we would triage it" and "Send this to your IT provider" are our interpretation of the sources, not a statement by CISA or the vendor.

Appendix 1. Severity decoded

CVE-2015-5477: score 7.5, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H` As the CVE record gives it. The record's own score can differ from the base score on the NVD record.

Metric	Value	What it means here
Attack vector	Network	Reachable over a network, with no need to be on the same segment.
Attack complexity	Low	No special conditions beyond the flaw itself.
Privileges required	None	No account is needed.
User interaction	None	No one has to do anything.
Scope	Unchanged	Damage stays inside the vulnerable component.
Confidentiality	None	No data exposed.
Integrity	None	Nothing can be altered.
Availability	High	Total loss of availability.

Appendix 2. Timeline

Date	Event
29 July 2015	CVE record published by Mitre.
8 October 2026	CISA added it to its list of exploited vulnerabilities.
11 October 2026	CISA's deadline for US federal agencies.

Appendix 3. Exposure by situation

These priorities are our judgement from the attacker prerequisites in the sources. They are not vendor ratings.

Your situation	Priority	Timeframe
A BIND server in the affected range answers queries from the internet	High	Now; CISA's deadline has passed
A BIND server in the affected range is reachable only from your internal network	Medium	This week
A router or appliance may embed BIND and the vendor has not said	Medium	This week, once the vendor replies

A BIND server outside the affected range	Low	Next patch cycle, record the version
You run no BIND	None	None for this CVE

Appendix 4. Definition of done

- Every ISC BIND you run is listed, with its version.
- Each is outside the affected list, or the vendor's mitigation is in place.
- The version output or a screenshot is saved with the date.
- Logs for the weeks before the update were searched, and anything odd was written down.
- Anything not done has an owner and a date.

Sources

- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- CVE record for CVE-2015-5477: https://www.cve.org/CVERecord?id=CVE-2015-5477
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Reference in the CVE record: h20564.www2.hpe.com: https://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c04789415
- Reference in the CVE record: kb.juniper.net: https://kb.juniper.net/JSA10783
- Reference in the CVE record: security.netapp.com: https://security.netapp.com/advisory/ntap-20160114-0001/
- Reference in the CVE record: kb.isc.org: https://kb.isc.org/article/AA-01438
- Reference in the CVE record: h20566.www2.hpe.com: https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05095918