CVE-2021-25218: A too-strict assertion check could be triggered when responses in BIND 9.16.19 and 9.17.16 require UDP fragmentation if RRL is in use

Updated on 19 Aug 2021 • 3 Minutes to read • Contributors

CVE: CVE-2021-25218 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-25218)

Document version: 2.0

Posting date: 18 August 2021

Program impacted: BIND

Versions affected: BIND 9.16.19, 9.17.16. Also, version 9.16.19-S1 of BIND Supported Preview Edition

Severity: High

Exploitable: Remotely

Description:

If `named` attempts to respond over UDP with a response that is larger than the current effective interface maximum transmission unit (MTU), and if response-rate limiting (RRL) is active, an assertion failure is triggered (resulting in termination of the `named` server process).

There are two ways for `named` to exceed the interface MTU:

- Direct configuration in `named.conf` setting `max-udp-size` to a value larger than the interface's MTU, or
- Path MTU discovery (PMTUD) informing the IP stack that it should use a smaller MTU for the interface and destination than the default `max-udp-size` value of 1232. Some operating systems allow packets received via other protocols to affect PMTUD values for DNS over UDP.

While RRL is not enabled by default for user-defined views or the built-in default INTERNET (IN) class view, "_default", the built-in default CHAOS (CH) class view, "_bind", does have RRL enabled.

Note that while this defect can be triggered through misconfiguration or by deliberate exploitation, it can also arise during normal operating conditions, even with hardened PMTUD settings.

Impact:

When a vulnerable version of named receives a query under the circumstances described above, the named process will terminate due to a failed assertion check.

The vulnerability affects only BIND 9 releases 9.16.19, 9.17.16, and release 9.16.19-S1 of the BIND Supported Preview Edition.

CVSS Score: 7.5

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

For more information on the Common Vulnerability Scoring System and to obtain your specific environmental score please visit: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H&version=3.1 (https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H&version=3.1)

Workarounds:

Disabling RRL in all views, including the built-in CHAOS class view "_bind", prevents the faulty assertion from being reached. This can be done by removing all existing `rate-limit` statements from `named.conf`, and defining a replacement for the default CHAOS view:

Text | Copy

```
view override_bind chaos {
        recursion no;
        notify no;
        allow-new-zones no;
        max-cache-size 2M;

        zone "version.bind" chaos {
                type primary;
                database "_builtin version";
        };
        zone "hostname.bind" chaos {
                type primary;
                database "_builtin hostname";
        };
        zone "authors.bind" chaos {
                type primary;
                database "_builtin authors";
        };
        zone "id.server" chaos {
                type primary;
                database "_builtin id";
        };
};
```

Active exploits:

We are not aware of any active exploits.

Solution:

Upgrade to the patched release most closely related to your current version of BIND:

- BIND 9.16.20
- BIND 9.17.17

BIND Supported Preview Edition is a special feature preview branch of BIND provided to eligible ISC support customers.

- BIND 9.16.20-S1

Document revision history:

1.0 Advance notification to customers, 11 August 2021

2.0 Public disclosure, 18 August 2021

Related documents:

See our **BIND 9 Security Vulnerability Matrix** (https://kb.isc.org/docs/aa-00913) for a complete listing of security vulnerabilities and versions affected.

Do you still have questions? Questions regarding this advisory should go to **security-officer@isc.org**. *To report a new issue, please encrypt your message using security-officer@isc.org's PGP key which can be found here:* ***https://www.isc.org/pgpkey/*** *(https://www.isc.org/pgpkey/). If you are unable to use encrypted email, you may also report new issues at:* ***https://www.isc.org/reportbug/*** *(https://www.isc.org/reportbug/).*

Note:

ISC patches only currently supported versions. When possible we indicate EOL versions affected. (For current information on which versions are actively supported, please see **https://www.isc.org/download/** (https://www.isc.org/download/).)

ISC Security Vulnerability Disclosure Policy:

Details of our current security advisory policy and practice can be found in the ISC Software Defect and Security Vulnerability Disclosure Policy at **https://kb.isc.org/docs/aa-00861** (https://kb.isc.org/docs/aa-00861).

The Knowledgebase article **https://kb.isc.org/docs/cve-2021-25218** (https://kb.isc.org/docs/cve-2021-25218) is the complete and official security advisory document.

Legal Disclaimer:

Internet Systems Consortium (ISC) is providing this notice on an "AS IS" basis. No warranty or guarantee of any kind is expressed in this notice and none should be implied. ISC expressly excludes and disclaims any warranties regarding this notice or materials referred to in this notice, including, without limitation, any implied warranty of merchantability, fitness for a particular purpose, absence of hidden defects, or of non-infringement. Your use or reliance on this notice or materials referred to in this notice is at your own risk. ISC may change this notice at any time. A stand-alone copy or paraphrase of the text of this document that omits the document URL is an uncontrolled copy. Uncontrolled copies may lack important information, be out of date, or contain factual errors.

Previous
CVE-2021-25219: Lame cache can be abused to severely degrade resolver performance

Next
CVE-2021-25216: A second vulnerability in BIND's GSSAPI security policy negotiation can be targeted by a buffer overflow attack