CVE-2021-3672

Missing input validation on hostnames returned by DNS servers

Project c-ares Security Advisory, August 10, 2021 - Permalink

VULNERABILITY

Missing input validation of host names returned by Domain Name Servers in the c-ares library can lead to output of wrong hostnames (leading to Domain Hijacking).

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2021-3672 to this issue.

STEPS TO REPRODUCE

An example domain which has a cname including a zero byte:

``` $ adig cnamezero.test2.xdi-attack.net

Answers: cnamezero.test2.xdi-attack.net. 0 CNAME victim.test2.xdi-attack.net\000.test2.xdi-attack.net. victim.test2.xdi-attack.net\000.test2.xdi-attack.net. 0 A 141.12.174.88 ```

When resolved via a vulnerable implementation, the CNAME alias and name of the A record will seem to be `victim.test2.xdi-attack.net` instead of `victim.test2.xdi-attack.net\000.test2.xdi-attack.net`, a totally different domain.

This is a clear error in zero-byte handling and can potentially lead to DNS-cache injections in case an application implements a cache based on the library.

### AFFECTED VERSIONS

This flaw exists in the following c-ares versions.

- Affected versions: c-ares 1.0.0 to and including 1.17.1
- Not affected versions: c-ares >= 1.17.2

### THE SOLUTION

In version 1.17.2, the function has been corrected and a test case have been added to verify.

A patch for CVE-2021-3672 is available.

### RECOMMENDATIONS

We suggest you take one of the following actions immediately, in order of preference:

A - Upgrade c-ares to version 1.17.2

B - Apply the patch to your version and rebuild

### TIME LINE

It was reported to the c-ares project on June 11, 2021 by Philipp Jeitner and Haya Shulman, Fraunhofer SIT.

c-ares 1.17.2 was released on August 10 2021, coordinated with the publication of this advisory.

### CREDITS

Thanks to Philipp Jeitner and Haya Shulman, Fraunhofer SIT for the report.
```