CVE-2014-0591: FAQ and Supplemental Information

Author: Reference Number: **AA-01085** Views: **51653** Created: **2014-01-13 18:50** Last Updated: **2014-12-12 21:17** **0 Rating**/ Voters

This page provides supplemental information for the CVE-2014-0591 Security Advisory (CVE-2014-0591: A Crafted Query Against an NSEC3-signed Zone Can Crash BIND.)

What causes this vulnerability?

One of our developers writes:

> "The bug (which causes an INSIST crash in name.c) is caused by a misuse of the standard memcpy() function which is, by happenstance, safe on most platforms: in this case a memory buffer was being copied to an overlapping buffer. The bug went undetected until recently because most implementations of memcpy() do handle this situation safely, but the standard does not require them to do so. Recent optimizations to glibc have removed the safetly net, exposing a long-existing but previously harmless coding error in named."

BIND is crashing on my system. How can I tell if this bug is the cause?

Nameservers crashing because of this bug will crash with an INSIST failure while checking a structure for consistency in name.c, usually between lines 1700 and 1800. The crash log message will look like this, although the exact line and message may vary depending on how the memcpy misuse has corrupted the structure.

```
name.c:1724: INSIST(count <= 63) failed
```

What systems are affected?

ISC is unable to characterize all of the systems affected but to date, every reporter who has encountered this bug has been running on a system using glibc 2.18. If you are running an operating system that does not use glibc for its system C library or if you are running a version prior to 2.18 you may not be vulnerable, though you can guarantee that you are not vulnerable by installing a version which patches the underlying memcpy() misuse. Whether or not the crash can occur depends on the behavior of your C library's memcpy() call.

Addendum, December 2014:

Red Hat Product Security advised us that they believe this problem might go back as far as glibc 2.11.

For assistance with problems and questions for which you have not been able to find an answer in our Knowledge Base, we recommend searching our community mailing list archives and/or posting your question there (you will need to register there first for your posts to be accepted). The bind-users and the dhcp-users lists particularly have a long-standing and active membership.

ISC relies on the financial support of the community to fund the development of its open source software products. If you would like to support future product evolution and maintenance as well having peace of mind knowing that our team of experts are poised to provide you with individual technical assistance whenever you call upon them, then please consider our Professional Subscription Support services - details can be found on our main website.