BIND9 - Denial of Service Exploit in the Wild

By Daniel Cid

Published: 2015-08-02 · Archived: 2026-04-05 23:17:46 UTC

BIND is one of the most popular DNS servers in the world. It comes bundled with almost every cPanel, VPS and dedicated server installation and is used by most DNS providers.

A week ago, the Internet Systems Consortium (ISC) team released a patch for a serious denial of service vulnerability (CVE-2015-5477) that allows a remote and unauthenticated attacker to crash the BIND (named) daemon, taking down a DNS server.

This happens because of an error in the way BIND handles TKEY queries, which with a single UDP packet can trigger a required assertion failure, causing the DNS daemon to exit.

Exploits in the Wild

Because of its severity we've been actively monitoring to see when the exploit would be live. We can confirm that the attacks have begun. DNS is one of the most critical parts of the Internet infrastructure, so having your DNS go down also means your email, HTTP and all other services will be unavailable.

If You Have Not Patched Your DNS Server, Do it Now!

All major Linux distributions (Redhat, Centos, Ubuntu, etc) have already provided patches for it and a simple **"yum update"** on Redhat/Centos or **"apt-get update"** on Debian-based systems will get you protected. Remember though, for the change to take affect you must restart BIND after the update.

If you run your own DNS server, a quick way to see if you are being targeted is to look for the "ANY TKEY" in your DNS logs:

> Aug 2 10:32:48 dns named[2717]: client a.b.c.d#42212 (foo.bar): view north_america: query: foo.bar ANY TKEY + (x.y.z.zz)

In fact, you can look for any type of **TKEY** request, as they are not very common, and see if there have been any attempts. The example above is from one of the public exploits released. Note that you need to have querylog enabled (which you can do with the command "**rndc querylog on**").

Clients using our DNS server, part of our Website Firewall, are already protected against this vulnerability. For existing customers, you can enable the use of our DNS manager and find instructions in our knowledgebase.

Related Tags

- DDoS

Source: https://blog.sucuri.net/2015/08/bind9-denial-of-service-exploit-in-the-wild.html