Mitigating BIND CVE-2015-5477 with iRules

MegaZone, 2015-25-09

While **SOL16909**: BIND vulnerability CVE-2015-5477 is the official SOL, and the best mitigation is, of course, upgrading to a fixed versions of TMOS, what if you can't upgrade right now?

One option is to not use BIND at all. The risk from CVE-2015-5477 is only present when BIND is used to resolve queries. If you use WIPs, DNS Caching, DNS Express, etc., and avoid BIND entirely, then you remove all risks associated with BIND. BIND should be the last option, and not just for security but also for performance. The other options will outperform BIND by a wide margin; DNS Express is 'baked in' to TMM and is vastly higher in performance than BIND. Don't overlook the better options just because BIND is familiar.

But what if moving off BIND is just not an option at this time? If you're on 10.x, I'm sorry to say there isn't much you can do. In theory you could write an iRule which did a binary scan, looking for DNS TKEY requests by byte, but this would be a *very* heavyweight solution and it is not something we can recommend. So if you're on 10.x we can only recommend upgrading to 10.2.4 HF12, or to 11.x or 12.x. (Which is a good idea anyway, as all 10.x releases hit End of Software Development at the end of the year; see SOL5903. That will mean no more code updates - no bug fixes, no security patches, nothing.)

If you're on 11.0.0 or later however, then you're in luck. 11.0.0 introduced the DNS::* iRule commands and that gives us some options for dealing with the CVE via iRules. Let's look at three options:

The first option is the simplest. If you don't have any need to serve TKEY records, and most sites do not, then you can simply drop any incoming TKEY requests.

```
when DNS_REQUEST {
    if {[DNS::question type] equals "TKEY" }{
        #log local0. "query [DNS::question name] type  [DNS::question type] dropped "
        drop
    }
}
```

The second option is a small variation on the first, to be a more RFC compliant. Instead of silently dropping the request it returns NOTIMPL to the query.

```
    if {[DNS::question type] equals "TKEY" }{
        #log local0. "query [DNS::question name] type  [DNS::question type] dropped "
        DNS::header rcode NOTIMPL
        DNS::return
    }
}
```

Finally, the third option is for those who do need to handle TKEY queries. This iRule examines the incoming TKEY queries and drops only those that appear to be CVE-2015-5477 DoS queries. This is the 'heaviest' of the three options as it does inspect every TKEY query.

```
when DNS_REQUEST {
    if {[DNS::question type] equals "TKEY" }{
```

```
        #log local0. "pkt qname [DNS::question name]"
        set rrs [DNS::additional]
        foreach rr $rrs {
            #log local0. "ar qname: [DNS::name $rr]"
            if {[DNS::type $rr] != 249 && [DNS::name $rr] == [DNS::question name]} {
                #log local0. "match"
                #log local0. "query [DNS::question name] type  [DNS::question type] dropped "
                DNS::header rcode NOTIMPL
                DNS::return
            }
        }
    }
}
```

There are some caveats to using iRules:

v10.0.0-v10.2.4:

- The DNS::* iRule Commands are **not** available - see above. iRules are not recommended.
- TMSH can be used to create and add an iRule to a GTM listener
- LTM module must be provisioned (but does not need to be licensed) if you want to use the GUI to create and add an iRule to a GTM listener

v11.0.0:

- The DNS::* iRule Commands are **read only**. That means only the first iRule above will work.
- TMSH can be used to create and add an iRule to a GTM listener
- LTM module must be provisioned (but does not need to be licensed) if you want to use the GUI to create and add an iRule to a GTM listener

v11.1.0-v11.4.1:

- TMSH can be used to create and add an iRule to a GTM listener
- LTM module must be provisioned (but does not need to be licensed) if you want to use the GUI to create and add an iRule to a GTM listener

v11.5.0+:

- TMSH can be used to create and add an iRule to a GTM listener
- GTM GUI can be used to create an iRule and add it to a GTM listener (TMUI > DNS > Delivery > iRules)

Again, the best option is to not use BIND at all, or, if you must use BIND, upgrade to a patched version as indicated in SOL16909. But if neither of those are viable options for you at this time, perhaps one of these iRules will provide you with a viable solution until you can take more permanent steps.

Thank you to Mark Lloyd, David Karakas, Lenz Yu, Hiroki Inoue, Kathleen McMonigal, and all of my colleagues in support and development who contributed to these solutions.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc. Corporate Headquarters info@f5.com	F5 Networks Asia-Pacific apacinfo@f5.com	F5 Networks Ltd. Europe/Middle-East/Africa emeainfo@f5.com	F5 Networks Japan K.K. f5j-info@f5.com