密级	内部

CVE-2015-5477-BIND 查询拒绝服务漏洞报告

[第一版 2015-08-05 下午]

北京知道创宇信息技术有限公司

监控预警中心

2015-08-05

1. 更新情况

版本	时间	描述
第一版	2015-08-05 下午	第一版完成

2. 漏洞描述

ISC BIND 是美国 Internet Systems Consortium（ISC）公司所维护的一套 DNS 域名解析服务软件。该软件被披露存在拒绝服务漏洞，由于 TKEY 查询的错误可导致 BIND 服务器发生 REQUIRE 断言失败并停止服务，攻击者利用漏洞可恶意构造数据包，导致 TKEY 记录查询错误，进而导致 BIND 服务器发生 REQUIRE 断言失败并停止服务。CNVD 对该漏洞的综合评级为“高危”。

漏洞影响 BIND 9 所有版本(包括 BIND 9.1.0 版本至 BIND 9.9.7-P1，BIND 9.10.0 至 BIND 9.10.2-P2 版本)，互联网上对应版本的递归服务器和权威服务器均受到该漏洞影响。根据实际使用情况评估，尽管 TKEY 查询功能使用较少，但由于基于漏洞构造的恶意攻击包有可能存在极强的前置条件，即使在服务器上配置访问控制列表或限制（拒绝）相关配置选项，也不能有效防范漏洞攻击。

BIND 查询拒绝服务漏洞能让黑客远程非授权对 BIND 所在服务器进行攻击，直至该 DNS 服务器崩溃，因为 BIND 句柄的 TKEY 查询中出现了 bug，一个简单的 UDP 包就可以导致 BIND 服务器出现“assertion failure”错误，进而服务器上的 DNS 服务守护进程会结束。

DNS 服务器使用方建议查找 DNS 日志里有没有“ANY TKEY”之类的关键词来判断是否该漏洞。

示例 DNS 攻击日志如下：

```
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)
```

上面的日志例子就是一个黑客 EXP 留下的信息。这还需要通过 rndc

querylog on 命令启用 querylog 来实现。

3. 影响范围

2015 年 8 月初，知道创宇 ZoomEye 团队对全国 DNS 服务器进行了摸底探测，发现国内共有 420084 台 DNS 服务器。其中使用 ISC BIND 服务的服务器有 29,913 台，占总量的 7.1%。

我国使用 ISC BIND 的服务器占全国比例已达到 7.1%，对我国基础网络稳定有较大的威胁，一旦遭受网络攻击将引发 dns 服务异常，从而会导致大范围网络中断。

3.1 使用 ISC BIND 的服务器地域分布

使用 ISC BIND 的服务器地域分布 TOP10 如图 1 所示。

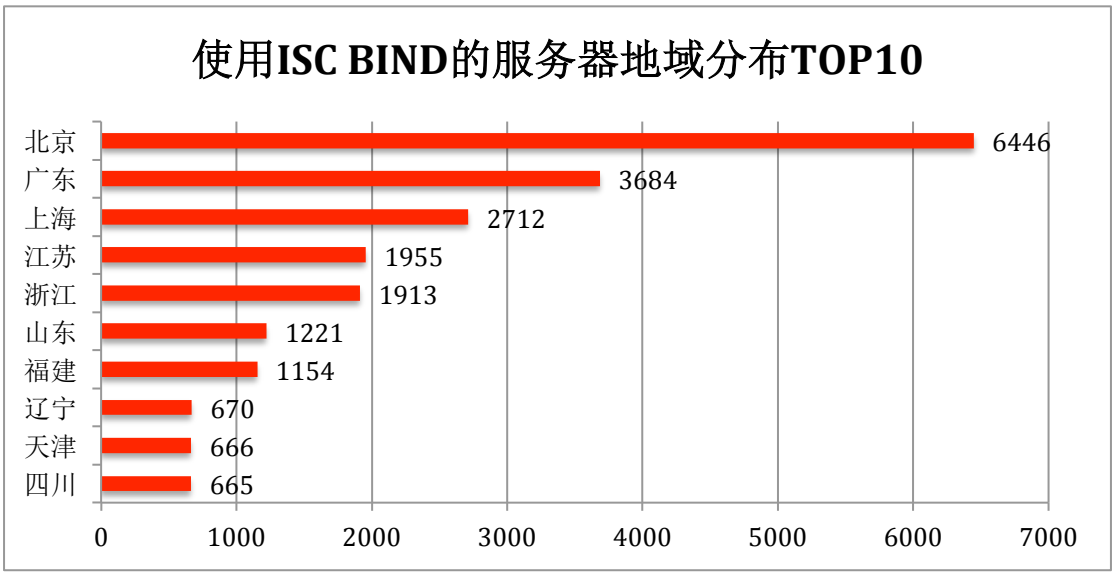

图 1 使用 ISC BIND 的服务器地域分布 TOP10

我国使用 ISC BIND 的服务器地域分布前五名分别是：北京 6,446 台 （占我国使用 ISC BIND 的服务器总数的 21.55%），广东 3,684 台(占比 12.3%），上海 2,712 台（占比 9.07%），江苏 1，955 台（占比 6.54%），浙江 1，913 台（占比 6.40%）。

全国 DNS 服务器 ISC BIND 使用率 TOP10，如图 2 所示：

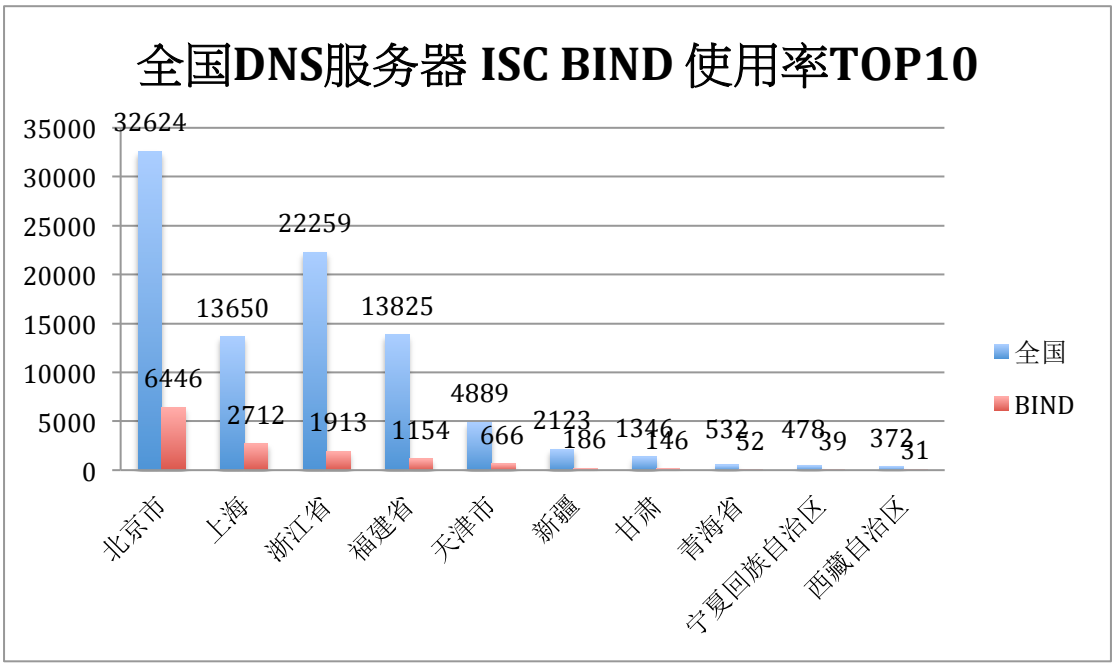

图 2 全国 DNS 服务器 ISC BIND 使用率 TOP10

目前，我国 DNS 的服务器地域分布中，北京、上海、浙江等地服务器使用 ISC BIND 服务占比较高，一旦遭受攻击，大量使用 ISC BIND 服务的城市将会有严重的网络瘫痪。

3.2 使用 ISC BIND 的服务器版本分布

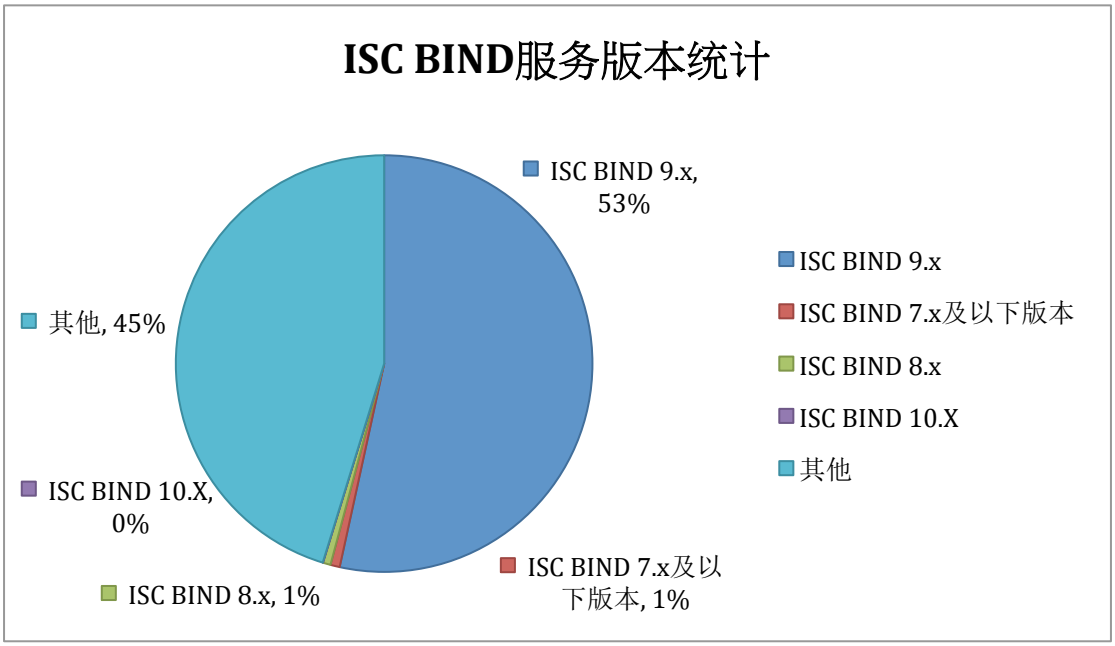

图 3 使用 ISC BIND 的服务器版本比例

3.3 使用 ISC BIND 服务的网络服务提供商分布

我国 DNS 服务器网络服务提供商分布如图 4 所示：

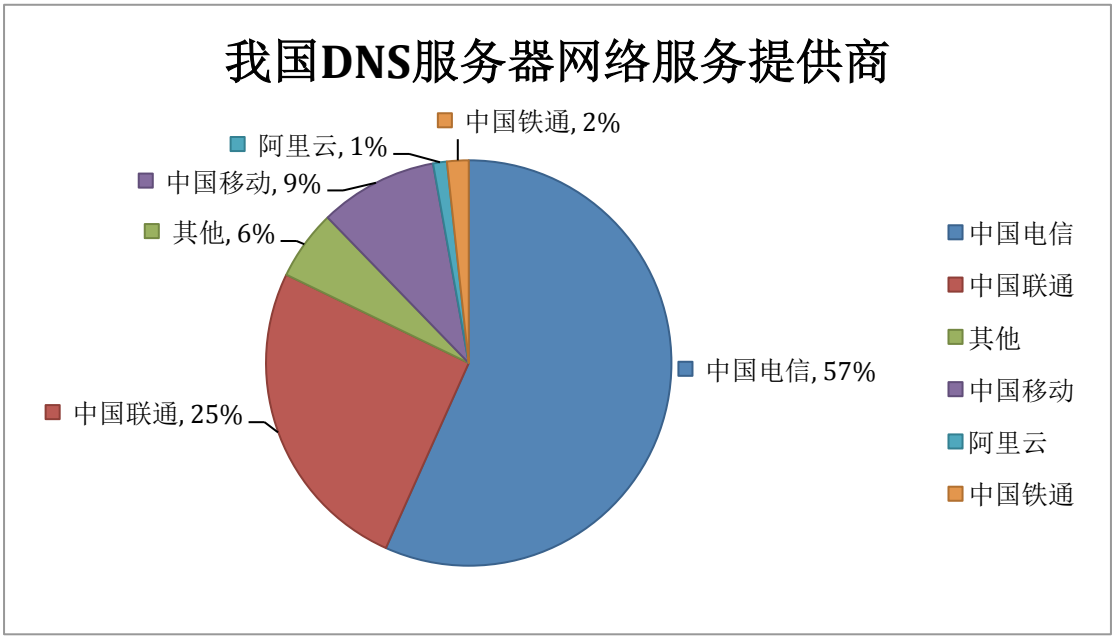

图 4 我国 DNS 服务器网络服务提供商分布

而使用 ISC BIND 服务的网络服务提供商分布如图 5 所示。

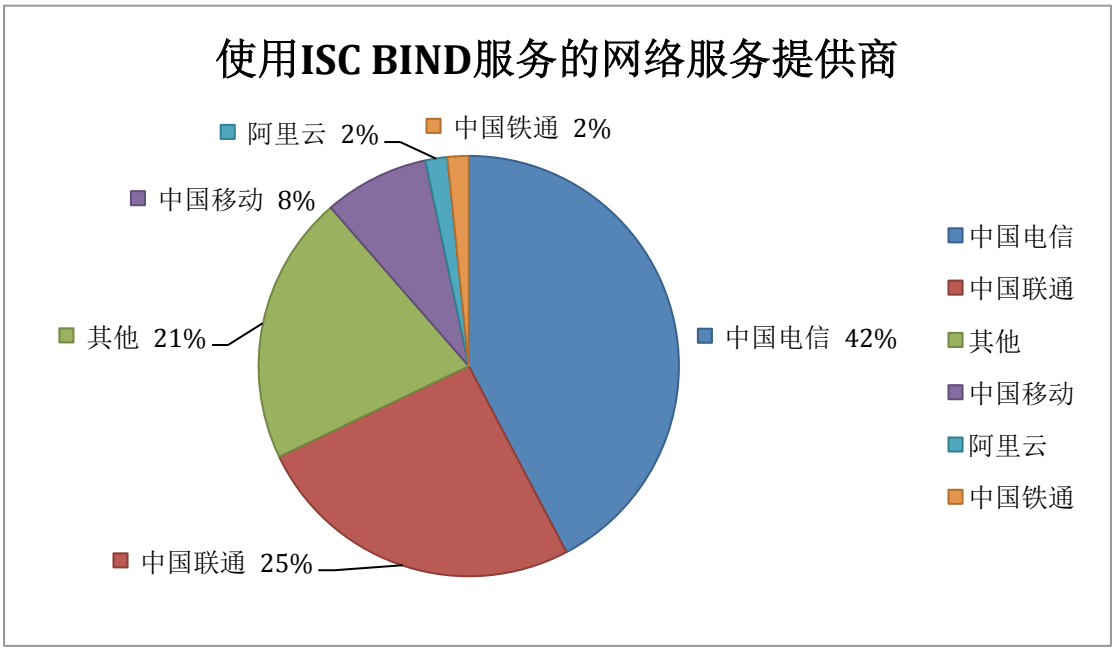

图 5 使用 ISC BIND 服务的网络服务提供商比例

由以上统计比例可知，我国使用 ISC BIND 的网络服务提供商中，前三名分别是中国电信（占比 42%）、中国联通（占比 25%）和中国移动（占比 8%），以上三家网络服务提供商的在我国拥有大量用户，一旦黑客发起大规模攻击，电信、联通服务器首当其冲将会引发连锁反应。

4. 解决方案

目前， 厂商已经发布了漏洞修补程序。知道创宇提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。建议相关用户升级到 BIND 最新版本。

下载地址：http://www.isc.org/downloads。