山西省互联网网络安全预警信息通报

2020年第3期（总第3期）

山西省通信管理局
主办：国家计算机网络应急技术处理协调中心山西分中心　　2020年5月31日

关于ISC BIND存在拒绝服务漏洞的安全公告

近日，国家信息安全漏洞共享平台（CNVD）收录了DNS BIND拒绝服务漏洞（CNVD-2020-29429）。攻击者利用该漏洞，可使BIND域名解析服务崩溃。目前，该漏洞的利用代码已公开，厂商已发布新版本完成修复。

一、漏洞情况分析

BIND（BerkeleyInternet Name Domain）是由美国互联网系统协会（ISC，Internet Systems Consortium）负责开发和维护的域名解析服务（DNS）软件，是现今互联网上使用较为广泛的DNS解析服务软件。

2020年5月22日，国家信息安全漏洞共享平台（CNVD）收录了由北京知道创宇信息技术股份有限公司报送的ISC BIND拒绝服务漏洞。由于BIND代码会对TSIG资源记录消息

进行正确性检查，因此攻击者可通过发送精心构造的恶意数据，使其进程在 tsig.c 位置触发断言失败，导致 BIND 域名解析服务崩溃。攻击者利用漏洞可发起拒绝服务攻击。该漏洞对互联网上广泛应用的 BIND 软件构建的域名服务器构成安全运行风险。

CNVD 对该漏洞的综合评级为“高危”。

二、漏洞影响范围

该漏洞影响的产品版本如下:

BIND 9.12.0 - 9.12.4P2

BIND 9.14.0 - 9.14.11

BIND 9.16.0 - 9.16.2

BIND 9.17.0 - 9.17.1 实验版本分支

BIND 9.13 - 9.15 所有废弃的开发分支

BIND 9.9.3-S1 至 9.11.18-S1 的发行预览版

三、处置措施

目前，BIND 官方已发布 9.11.19，9.14.12 及 9.16.3 版本完成漏洞修复，CNVD 建议用户关注厂商主页，尽快升级至新版本，避免引发漏洞相关的网络安全事件。

参考链接:

https://www.isc.org/downloads/bind/（补丁地址）

https://downloads.isc.org/isc/bind9/9.11.19/BIND9.11.19.x64.zip

https://downloads.isc.org/isc/bind9/9.14.12/BIND9.14.12.x64.zip

https://downloads.isc.org/isc/bind9/9.16.3/BIND9.16.3.x64.zip