山西省互联网网络安全预警信息通报

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　2018 年 2 月 21 日

关于 MongoDB 数据库不当配置导致信息泄露风险情况通报

2 月 14 日，CNCERT 监测发现，我国境内部分 MongoDB 数据库暴露在互联网上导致重要信息泄露。经进一步排查，我国境内互联网上使用 MongoDB 数据库服务的 IP 地址有约 2.5 万个，其中存在信息泄露风险的 IP 地址有 468 个。具体情况如下：

一、MongoDB 数据库不安全配置情况

通过分析发现，在 MongoDB 数据库启动时，如不修改数据库认证访问权限方面的默认配置，用户则无需权限验证，通过默认的服务端口可以本地或远程访问该数据库并进行任意操作。此类数据库若暴露在互联网上，可能存在信息泄露风险。

二、MongoDB 数据库排查和处置情况

CNCERT 在发现 MongoDB 数据库存在的安全隐患后，及时对我国存在类似情况的数据库进行了排查。CNCERT 抽样监测发现，截止 2 月 17 日，我国境内互联网上使用 MongoDB 数据库服务的 IP 地址有约 2.5 万个，其中存在信息泄露风险的 IP 地址有 468 个，涉及山西省的 IP 有 3 个。这些存在信息泄露风险的 IP 地址分布在我国境内 28 个省份，北京、广东、上海的 IP 地址数量排名前三；部分数据库涉及我国交通、煤矿等重要行业；在云服务商平台上搭建的数据库服务的数量占比超过 40%。

为尽快消除安全风险，山西分中心对存在信息泄露风险的数据库进行逐个核查，并通知数据库运营者尽快修复相关问题。

三、处置建议

针对国内 MongoDB 数据库用户，建议采取以下措施加强防护:

（一）检查使用 MongoDB 数据库配置情况，对其默认配置进行修改，包括修改默认服务器端口、创建管理账号并配置用户认证权限。

（二）尽量不要将 MongoDB 数据库部署在互联网上，并对访问数据库 IP 地址采取限制等措施。