2016 年 9 月 30 日，星期五

漏洞聚焦：Redis CONFIG SET client-output-buffer-limit 代码执行漏洞

漏洞发现者：Talos 团队的 Cory Duplantis

概述

Talos 公开了 Redis 中发现的越界写入漏洞 TALOS-2016-0206/CVE-2016-8339。Redis 是使用键值模型的简单内存数据结构存储系统。其他数据库无法解决的问题，或者因为内在原因导致处理缓慢的问题，都可以通过 Redis 处理，因此 Redis 越来越受欢迎。本文中讲的这个漏洞存在于 Redis 数据结构存储系统使用 CONFIG SET 命令处理 client-output-buffer-limit 选项的过程中。攻击者精心设计的 CONFIG SET 命令能引发越界写入，进而可能会导致代码执行。

详细信息

Redis 在使用“CONFIG SET”命令修改“client-output-buffer-limit”选项时，存在一个越界写入漏洞。设置“client-output-buffer-limit”选项所需的语法如下所示。

```
CONFIG SET client-output-buffer-limit <class> <hard limit> <soft limit> <soft seconds>
```

此选项通过设置限制，实现断开某类客户端连接的目的。在解析“client-output-buffer-limit”时，系统会通过调用“getClientTypeByName”获取对应类的类型。这时，“getClientTypeByName”会返回 [-1, 3] 范围内的一个值。通过“client_obuf_limits”阵列的声明，我们可以看到该阵列的大小为“3”。虽然“client-output-buffer-limit”预期得到的客户端类型只有“normal”、“slave”和“pubsub”，但“master”同样是有效客户端。通过提供客户端类“master”，可以对“client_obufs_limit”阵列造成数据溢出，进而致使之后的结构变量被覆盖。此漏洞可能导致远程代码执行，应得到相应处理。有关此漏洞的完整详情，请查看我们网站上的漏洞公告。

防护

以下 Snort 规则将会检测出漏洞攻击尝试。请注意，Talos 未来可能会发布更多规则，当前规则会根据未来得到的更多漏洞信息而有所变更。如需获取有关最新规则的信息，请参阅防御中心或 Snort.org。

Snort 规则：40301

发布者：NICK BIASINI；发布时间：12:11

标签：零日、REDIS、TALOS、漏洞研究、漏洞聚焦