2017 年 2 月 21 日，星期二

漏洞聚焦：Aerospike NoSQL 数据库服务器中发现多个漏洞

漏洞发现者：Talos

Talos 公布在 Aerospike 数据库服务器中发现了多个漏洞。这些漏洞包括从拒绝服务到潜在的远程代码执行。各类需要高性能 NoSQL 数据库的公司都在使用此软件。这些问题已经在 Aerospike 数据库软件的版本 3.11.1.1 中得到解决。

Aerospike 数据库服务器是一种可扩展的分布式 NoSQL 数据库，可用作需要键值存储的可扩展 Web 应用的后端。此服务器注重性能，采用多线程设计，并将索引完全保留在 RAM 中，同时能够将数据永久存储到固态驱动器或传统旋转介质中。

TALOS-2016-0263 (CVE-2016-9049) - Aerospike 数据库服务器 Fabric_Worker Socket-Loop 拒绝服务漏洞
TALOS-2016-0265 (CVE-2016-9051) - Aerospike 数据库服务器客户端批处理请求代码执行漏洞
TALOS-2016-0267 (CVE-2016-9053) - Aerospike 数据库服务器 RW Fabric Message Particle Type 代码执行漏洞

详细信息

拒绝服务漏洞

TALOS-2016263 是存在于 Aerospike 数据库服务器的 fabric-worker 组件中的 DoS 漏洞。经特殊设计的数据包可以使服务器进程取消引用空指针。攻击者只需连接到 TCP 端口即可触发此漏洞。

代码执行漏洞

TALOS-2016-0265 影响解析 Aerospike 数据库服务器功能的批处理事务字段。攻击者可以使用经特殊设计的数据包，利用越界写入引发可能导致远程代码执行的内存损坏。攻击者只需连接到侦听端口并发送经特殊设计的数据包，即可触发此漏洞。

TALOS-2016-0267 涉及 Aerospike 数据库服务器 RW Fabric Message Particle Type 中的一个越界索引漏洞。经特殊设计的数据包可能导致服务器在阵列边界外获取可能导致远程代码执行的函数表。攻击者只需连接到侦听端口即可触发此漏洞。

测试版本

Aerospike 数据库服务器 3.10.0.3

防护

以下 Snort 规则可以检测相关的漏洞攻击活动。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：41209、41213 和 41219

发布者：EARL CARTER；发布时间：11:22
标签：NOSQL、漏洞