2017 年 1 月 12 日星期四

漏洞聚焦：对 Aerospike 数据库服务器的攻击

漏洞发现者：Talos

Talos 公开了在 Aerospike 数据库服务器中发现的多个漏洞。这些漏洞包括从内存泄露到潜在的远程代码执行等多种漏洞。各类需要高性能 NoSQL 数据库的公司都在使用此软件。Aerospike 在版本 3.11 中修复了这些问题。

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-2016-0264 (CVE-2016-9050) - Aerospike 数据库服务器客户端消息内存泄露漏洞

TALOS-2016-0266 (CVE-2016-9052) - Aerospike 数据库服务器索引名称代码执行漏洞

TALOS-2016-0268 (CVE-2016-9054) - Aerospike 数据库服务器集名称代码执行漏洞

详细信息

内存泄露漏洞

TALOS-2016-0264 是 Aerospike 数据库服务器客户端消息解析功能中存在的可被利用的越界读取漏洞。攻击者可以通过向侦听端口发送经特殊设计的数据包，导致越界读取，进而造成在进程中发生内存泄露。此漏洞也可用于触发拒绝服务。

代码执行漏洞

TALOS-2016-0266 是 Aerospike 数据库服务器查询功能中存在的可被利用的基于堆栈的缓冲区溢出漏洞。攻击者利用经特殊设计的数据包，导致“as_sindex__simatch_by_iname”功能发生基于堆栈的缓冲区溢出，进而实现远程代码执行。攻击者只需连接到侦听端口，便可以触发此漏洞。

TALOS-2016-0268 会对 Aerospike 数据库服务器的查询功能造成影响。使用经特殊设计的数据包，攻击者可以利用“as_sindex__simatch_list_set_binid”功能中可被利用的基于堆栈的缓冲区溢出漏洞执行远程代码。攻击者只需要连接到侦听端口，便可以触发此漏洞。

测试版本

Aerospike 数据库服务器 3.10.0.3

防护

Aerospike 版本 3.11 解决了这些问题。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：41206、41212、41216

发布者：EARL CARTER；发布时间：15:01
标签：零日、AEROSPIKE、NOSQL、漏洞