2016 年 12 月 20 日，星期二

漏洞聚焦：Tarantool 拒绝服务漏洞

漏洞发现者：Talos

Talos 公开了 Tarantool 中的两个拒绝服务漏洞（CVE-2016-9036 和 CVE-2016-9037）。Tarantool 是基于 lua 的开源应用服务器。虽然其主要用作应用服务器，但也能提供类似数据库的功能，并提供一个内存数据库，可使用基于 MsgPack 序列化格式的协议查询该数据库。Mail.RU 或 Badoo 等多家运营商都使用 Tarantool。

详细信息

TALOS-2016-0254 (CVE-2016-9036) TARANTOOL MSGPUCK MP_CHECK 拒绝服务漏洞

Msgpuck 库用于编码和解码以 MsgPack 格式序列化的数据。此库最初实现为用于 Tarantool 应用服务器的序列化和反序列化默认库，但也作为独立库分发，为其他 C 或 C++ 应用提供对 MsgPack 格式的支持。

反序列化以 MsgPack 格式编码的数据时，Msgpuck 库提供一个名为“mp_check”的函数，用于在解码之前验证 Msgpack 数据。经特殊设计的数据包可能会导致“mp_check”函数在尝试检查解码 map16 数据包是否超出缓冲区范围时错误地返回成功消息，从而导致出现拒绝服务情况。

TALOS-2016-0255 (CVE-2016-9037) TARANTOOL 密钥类型拒绝服务漏洞

Tarantool 的协议基于 MsgPack 序列化格式。此协议用于编码随后对服务器发出的特定请求类型。该协议报头内部是编码为映射类型的数据，其中每个密钥用整数表示。每个整数用作索引，指向用于确定指定密钥类型的阵列。通过发送经特殊设计的数据包，攻击者可以使“xrow_header_decode”函数访问越界内存位置，进而造成服务器拒绝服务。

测试版本

Tarantool 1.7.2-0-g8e92715

Msgpuck 1.0.3

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：41080-41082

发布者：EARL CARTER；发布时间：14:27

标签：零日、TARANTOOL、漏洞