2017 年 10 月 31 日，星期二

漏洞聚焦：Cesanta Mongoose 服务器中的多个漏洞

这些漏洞是思科 Talos 的 Aleksandar Nikolic 发现的

今天，Talos 披露在 Cesanta Mongoose 服务器中发现的多个漏洞。

Cesanta Mongoose 是一个执行多个网络协议的库，其中包括 HTTP、MQTT 和 MDNS 等协议。它在设计方面充分考虑了嵌入式设备的要求，可用于众多物联网 (IoT) 设备，并且几乎可以在所有常用的物联网平台上运行。该软件占用内存较小，可以让任何互联网连接的设备作为一个 Web 服务器来运行。Mongoose 可在 GPL v2 和商业许可证下使用。
该库的 6.10 版本已修复所发现的这些漏洞。

漏洞详细信息

TALOS-2017-0398 (CVE-2017-2891) - Cesanta Mongoose HTTP 服务器 CGI 远程代码执行漏洞

TALOS-2017-0398 是 Cesanta Mongoose 6.8 的 HTTP 服务器实施中存在的一个可利用的 Use After Free 漏洞。以 CGI 为目标的普通 HTTP POST 请求会导致重新使用以前释放的指针，从而可能导致远程代码执行。攻击者需要通过网络发送此 HTTP 请求，以触发此漏洞。

TALOS-2017-0399 (CVE-2017-2892) - Cesanta Mongoose MQTT 负载长度远程代码执行漏洞

TALOS-2017-0399 是 Cesanta Mongoose 6.8 的 MQTT 数据包解析功能中存在的一个漏洞，攻击者可利用该漏洞读取任意内存。攻击者可使用经特殊设计的 MQTT 数据包，诱发越界错误和任意内存读写，进而造成信息泄露、拒绝服务和远程代码执行。攻击者需要通过网络发送经特殊设计的 MQTT 数据包，以触发此漏洞。

TALOS-2017-0400 (CVE-2017-2893) - Cesanta Mongoose MQTT SUBSCRIBE 命令拒绝服务

TALOS-2017-0400 是指 Cesanta Mongoose 6.8 的 MQTT 数据包解析功能中存在的一个可利用的 NULL 指针取消引用漏洞。攻击者可以利用 MQTT SUBSCRIBE 数据包诱发 NULL 指针取消引用，进而导致服务器崩溃和拒绝服务。攻击者需要通过网络发送经特殊设计的 MQTT 数据包，以触发此漏洞。

TALOS-2017-0401 (CVE-2017-2894) - Cesanta Mongoose MQTT SUBSCRIBE 多主题远程代码执行

TALOS-2017-0401 是 Cesanta Mongoose 6.8 的 MQTT 数据包解析功能中存在的一个可利用的堆栈缓冲区溢出漏洞。攻击者可以使用经特殊设计的 MQTT SUBSCRIBE 数据包诱发堆栈缓冲区溢出，从而远程执行代码。攻击者需要通过网络发送经特殊设计的 MQTT 数据包，以触发此漏洞。

TALOS-2017-0402 (CVE-2017-2895) - Cesanta Mongoose MQTT SUBSCRIBE 主题长度信息泄漏漏洞

TALOS-2017-0402 是 Cesanta Mongoose 6.8 的 MQTT 数据包解析功能中存在的一个可利用的任意内存读取漏洞。攻击者可以使用经特殊设计的 MQTT SUBSCRIBE 数据包诱发越界错误和任意内存读取，进而可能造成信息泄漏和拒绝服务。攻击者需要通过网络发送经特殊设计的 MQTT 数据包，以触发此漏洞。

TALOS-2017-0416 (CVE-2017-2909) - Cesanta Mongoose DNS 查询压缩名称指针拒绝服务漏洞

TALOS-2017-0416 是指 Cesanta Mongoose 6.8 库的 DNS 服务器功能中存在的一个无限循环编程错误。攻击者可使用经特殊设计的 DNS 请求诱发无限循环，进而造成 CPU 使用率过高并触发拒绝服务攻击。攻击者可以通过网络发送数据包来触发此漏洞。

TALOS-2017-0428 (CVE-2017-2921) - Cesanta Mongoose Websocket 协议包长度代码执行漏洞

TALOS-2017-0428 是指 Cesanta Mongoose 6.8 的 Websocket 协议实施中存在的一个可利用的内存损坏漏洞。攻击者可以使用经特殊设计的 Websocket 数据包诱发整数溢出，导致堆缓冲区溢出，进而实现拒绝服务攻击和可能的远程代码执行。攻击者可以通过网络发送经特殊设计的 Websocket 数据包，以触发此漏洞。

TALOS-2017-0429 (CVE-2017-2922) - Cesanta Mongoose Websocket 协议分段数据包代码执行漏洞

TALOS-2017-0429 是指 Cesanta Mongoose 6.8 的 Websocket 协议实施中存在的一个可利用的内存损坏漏洞。攻击者可使用经特殊设计的 Websocket 数据包使系统分配缓冲区，同时留下旧指针，从而可以利用 Use After Free 漏洞来实现远程代码执行。攻击者可以通过网络发送经特殊设计的 Websocket 数据包，以触发此漏洞。

有关这些漏洞的完整技术详细信息，请参阅我们网站上发布的漏洞公告：

http://www.talosintelligence.com/vulnerability-reports/

讨论

物联网设备通常仅具有有限的处理资源和内存资源，但它们也需要轻量级和弹性通信协议。物联网和移动消息应用经常使用的协议之一是 MQ 遥测传输 (MQTT)。

MQTT 是一种轻量级网络协议，可用于在不同设备之间发布/订阅消息。MQTT 是通过 OASIS 联盟认证用于采用开放标准的标准协议。

该协议开放、简单、易于实施。利用该协议，一台服务器可以支持数千个轻量级客户端。该协议试图在尽量减少带宽需求的同时，确保交付的可靠性。

Cesanta Mongoose 是一个常用的通信库，可作为一个轻量级嵌入式库实施，可支持多个服务器和客户端应用程序层协议，如 HTTP、MQTT、WebSocketDNS 和 CoAPCoAP。它在设计方面充分考虑了嵌入式设备的要求，可用于众多物联网 (IoT) 设备，并且几乎可以在所有常用的物联网平台上运行。

攻击者可利用 Talos 发现的这些漏洞来接管 Cesanta Mongoose 服务器易受攻击版本的实施，并控制各台设备以及运行这些设备的相关服务器。Talos 建议用户与受影响的设备供应商合作，确保将 Cesanta Mongoose 的最新安全补丁应用于所有易受攻击的设备和应用中。

防护

以下 Snort 规则可检测试图利用这些漏洞的行为。请注意，Talos 未来可能会发布更多规则，当前规则会根据以后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所有信息，请参阅 Firepower 管理中心或 Snort.org。

Snort 规则：

- 23039 - 23040

发布者：VANJA SVAJCER 发布时间：11:12 AM
标签：CESANTA、CVE-2017-2891、CVE-2017-2892、CVE-2017-2893、CVE-2017-2894、CVE-2017-2895、CVE-2017-2909、CVE-2017-2921、CVE-2017-2922、MONGOOSE、远程代码执行、漏洞聚焦