2016 年 10 月 31 日，星期一

漏洞聚焦：Memcached 中发现可被远程利用的漏洞（已修复）

漏洞发现者：Talos 团队的 Aleksandar Nikolich。

为增强互联网安全并保护客户，我们开展了多项工作，其中包括寻找和研究第三方软件中的零日漏洞。本着利用编程方法寻找漏洞，并以负责任的态度披露漏洞的精神，Talos 现披露在 Memcached 中发现的三个漏洞。Memcached 是一个开源的高性能分布式内存缓存系统，可帮助那些使用后台数据库的动态网站提高速度。目前，Memcached 已广泛用于各种在线应用。至于本文披露的漏洞，Memcached 开发人员已发布相关补丁加以修复。

漏洞详细信息

Memcached 中存在多个整数溢出漏洞。攻击者可利用这些漏洞在受攻击系统上实现远程执行代码的目的。这些漏洞在用于插入、尾端附加、前端附加或修改键/值数据对的许多 Memcached 函数中出现。另外，受 Memcached 处理 SASL 身份验证命令的方式影响，如果系统中使用的 Memcached 经过编辑，可以支持 SASL 身份验证，那么系统将很容易受到第三方漏洞攻击。

通过向受攻击服务器发送精心设计的 Memcached 命令，攻击者可以利用这些漏洞发动攻击。此外，攻击者还可以利用这些漏洞获取敏感进程信息，从而绕过普通的漏洞攻击缓解技术（例如 ASLR），并且这种情形可能会多次触发。这会让漏洞攻击更容易成功，因此这些漏洞的严重程度很值得重视。

强烈建议将 Memcached 服务器设置为只允许在受信任环境中访问；然而，许多 Memcached 服务器的设置却是允许通过互联网访问。另外，即便 Memcached 部署在“受信任”环境中，管理员也不能掉以轻心。因为攻击者对有漏洞的服务器发动攻击后，可以在网络中横向移动。

Talos 在 Memcached 中发现的漏洞列表如下：

- TALOS-2016-0219 - Memcached 服务器尾端附加/前端附加远程代码执行漏洞
- TALOS-2016-0220 - Memcached 服务器更新远程代码执行漏洞
- TALOS-2016-0221 - Memcached 服务器 SASL 身份验证远程代码执行漏洞

有关每个漏洞的更多详情，请参见链接中的漏洞报告，或访问我们网站的“漏洞报告”(Vulnerability Report) 门户：

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

开展深入研究，发现第三方软件中的漏洞是 Talos 将长期坚持的任务，这不仅是为了保护我们的客户，也是为了整体改善互联网安全状况。开发编程方法来发现漏洞，本着负责任的态度披露发现的漏洞，并确保漏洞得到修复是我们工作的关键。通过此研究工作，我们能够保护软件安全，避免软件遭到攻击者利用，并深入了解如何帮助改善开发实践。

防护

以下 Snort 规则能够检测试图利用我们所披露的 Memcached 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所有信息，请参阅 FireSIGHT 管理中心或 Snort.org。

Snort 规则：40468-40483

发布者：ALEXANDER CHIU；发布时间：15:53
标签：MEMCACHED、补丁、漏洞研究