2017 年 5 月 12 日，星期五

漏洞聚焦：Hangul Word Processor 远程代码执行漏洞

漏洞发现者：Talos 团队的 Rich Johnson。

简介

由 Hancom inc. 发布的 Hangul Office Suite（包含 Hangul Word Processor）是韩国领先的文字处理和办公生产力套件。攻击者可利用此漏洞制作一个恶意文档，该文档打开后，攻击者可在受害者的系统中执行任意代码。

TALOS-2017-0320 (CVE-2017-2819) Hangul Word Processor 缓冲区溢出漏洞

Hangul Word Processor 文档使用结构化格式存储包括最终文档在内的各种对象。当打开文档时，该软件读取描述对象属性的元数据标签，并计算存储每个对象所需的内存。
记录 HWPTAG_TAB_DEF 描述有关文档中标签定义的信息。此部分中的标头信息描述加载相关数据部分需要多少内存，不过，可以在标头中加入一个值，使得之前的标签定义中使用的堆缓冲区在未调整大小的情况下被重复使用。这会导致缓冲区溢出的情况（因为标签部分的内容写在堆中已分配缓冲区之外），最终导致远程代码执行。

更多信息请查看漏洞报告：TALOS-2017-0320。

了解易受攻击的版本：Hancom Office 2014 版本 9.1.0.2172

讨论

Hangul Wor Processor 文档是攻击韩国用户的威胁发起者最喜欢用的媒介。我们最近编写了此类威胁的两个示例，请在此处和此处查看。办公生产力软件中的漏洞对攻击者而言非常有用，他们可以利用通过邮件频繁分发的文件格式，锁定要攻击的对象。用户应确保持续更新所有软件（包括办公生产力套件）的补丁，从而确保攻击者无法利用这些漏洞危害系统。

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：35832 - 35833

发布者：MARTIN LEE 发布时间：9:22
标签：缓冲区溢出、CVE-2017-2819、HANGUL、漏洞、漏洞聚焦