2017 年 5 月 4 日，星期四

漏洞聚焦：AntennaHouse DMC 库任意代码执行漏洞

漏洞发现者：思科 Talos 团队的“冰壁”Marcin Noga。

今天，Talos 披露了在 AntennaHouse DMC 库中发现的多个漏洞，该库在各种产品中广泛用于基于 Web 的文档搜索和渲染。出现这些漏洞是因为无法正确解析 Microsoft Office 文档，攻击者可利用这些漏洞实现任意代码执行。Talos 与 AntennaHouse 共同披露了这些漏洞。

漏洞详细信息

AntennaHouse DMC HTMLFilter 中存在多个堆损坏漏洞。攻击者可利用这些漏洞在目标计算机上实现任意代码执行。出现这些漏洞是因为对 Microsoft Office 文档（例如 Word 和 PowerPoint 文件）处理不当。攻击者可通过向转换器传送经特殊设计的文档，利用其中一个漏洞。值得注意的是，众所周知，该库会集成到其他第三方产品中，因此攻击者入侵易受攻击的计算机的方法多种多样。

有关这些漏洞的完整技术详细信息，请参阅以下完整漏洞公告：

- TALOS-2016-0207 (CVE-2016-8382) - AntennaHouse DMC HTMLFilter Doc_SetSummary 代码执行
- TALOS-2016-0208 (CVE-2016-8383) - AntennaHouse DMC HTMLFilter Doc_GetFontTable 代码执行
- TALOS-2016-0209 (CVE-2016-8384) - AntennaHouse DMC HTMLFilter DHFSummary 代码执行
- TALOS-2017-0279 (CVE-2017-2783) - AntennaHouse DMC HTMLFilter FillRowFormat 代码执行漏洞
- TALOS-2017-0284 (CVE-2017-2792) - AntennaHouse DMC HTMLFilter iBldDirInfo 代码执行漏洞
- TALOS-2017-0285 (CVE-2017-2793) - AntennaHouse DMC HTMLFilter UnCompressUnicode 代码执行漏洞
- TALOS-2017-0286 (CVE-2017-2794) - AntennaHouse DMC HTMLFilter PPT DHFSummary 代码执行漏洞
- TALOS-2017-0288 (CVE-2017-2795) - AntennaHouse DMC HTMLFilter Txo 代码执行漏洞
- TALOS-2017-0290 (CVE-2017-2797) - AntennaHouse DMC HTMLFilter PPT ParseEnvironment 代码执行漏洞

- TALOS-2017-0291 (CVE-2017-2798) - AntennaHouse DMC HTMLFilter GetIndexArray 代码执行漏洞
- TALOS-2017-0292 (CVE-2017-2799) - AntennaHouse DMC HTMLFilter AddSst 代码执行漏洞

防护

为了保护我们的客户，Talos 已经发布了相关规则来检测利用这些漏洞的攻击尝试。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：40789-40790、40927-40932、41511-41512、41543-41546、41703-41704、41726-41727、41753-41754、41759-41760、41765-41766

有关以上漏洞和其他漏洞的完整技术详细信息，请访问我们网站上的漏洞报告门户：

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

发布者：ALEXANDER CHIU；发布时间：13:09
标签：ANTENNAHOUSE、SNORT 规则、漏洞研究