2016 年 11 月 17 日，星期四

漏洞聚焦：经过修复的 HDF5 文件库中存在多个文件解析漏洞

漏洞发现者：Talos 漏洞研究团队。

今天，Talos 公布了在 HDF5 中发现的四个漏洞。HDF5 是一种用于存储和组织大量科学数据的文件格式，也用于在应用之间进行数据交换。在 GIS 行业，人们通过库（如 GDAL、OGR）使用它，或者将其用作软件（如 ArcGIS）的一部分。HDF5 由非盈利组织 HDF 小组维护，Talos 曾与该组织合作，确保以负责任的方式公开这些漏洞。HDF5 版本 1.8.18 修复了这些漏洞。

以下是已发现并修复的漏洞列表：

- CVE-2016-4330 (TALOS-2016-0176) - HDF5 小组 libhdf5 H5T_ARRAY 代码执行漏洞
- CVE-2016-4331 (TALOS-2016-0177) - HDF5 小组 libhdf5 H5Z_NBIT 代码执行漏洞
- CVE-2016-4332 (TALOS-2016-0178) - HDF5 小组 libhdf5 可分享消息类代码执行漏洞
- CVE-2016-4333 (TALOS-2016-0179) - HDF5 小组 libhdf5 H5T_COMPOUND 代码执行漏洞

漏洞详细信息

TALOS-2016-0176

此漏洞存在的方式为，HDF 无法检查已读取阵列的维数，从而无法确认文件是否在为其分配的空间边界内。在将文件中的元素读入阵列时，会发生基于的堆缓冲区溢，从而导致在应用使用该库的情况下可能会出现任意代码执行。

TALOS-2016-0177

当库将数据从使用 H5Z_NBIT 编码的数据集中解码出来时，存在缓冲区溢出漏洞。在计算编码 BCD 数字的精度时，此库将无法进行边界检查，导致其在为此 BCD 数字分配的空间边界之外计算索引。然后，此库将在缓冲区边界之外写入数据，导致基于的堆缓冲区溢出并可能造成代码执行。

TALOS-2016-0178

存在此漏洞的原因是库无法检查特定消息类型是否支持特定标志。当设置了此标志时，库会将结构投到备用结构，并将其分配给不受此消息类型支持的字段。此消息类型无法支持此标志，且库将在堆缓冲区的边界之外写入数据，从而导致代码执行。

TALOS-2016-0179

此报告详细介绍了解析 HDF 文件时 H5O_dtype_decode_helper 程序中出现的基于堆的缓冲区溢出。由于在解析文件时未对内存中特定值进行充分处理，当用户打开经过特殊设计的 HDF 文件时，则可以在应用使用此库的情况下利用此漏洞并实现代码执行。

有关这些漏洞的完整详细信息，请访问我们的漏洞报告：

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

覆盖范围

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：40791-40794、40801-40810

发布者：ALEXANDER CHIU；发布时间：23:20
标签：HDF5、补丁、SNORT 规则、漏洞报告