2016 年 3 月 31 日，星期四

漏洞聚焦：LHASA 整数下溢漏洞

漏洞发现者：Marcin Noga，思科 Talos 团队。

Talos 宣布在 Lhasa LZH/LHA 解压工具和库中发现漏洞 TALOS-2016-0095/CVE-2016-2347。此漏洞的原因是特定整数下溢情况。该软件会验证标头值是否过大，但是不会验证标头长度是否过短。如果对标头大小过小的 LHA 或 LZH 文件执行解压，就会导致解压软件分配一个指向已释放的堆内存的指针。攻击者通过控制这类文件的长度和内容，就能利用该漏洞以任意代码覆盖堆内存。

例如，攻击者可以诱骗用户打开恶意文件，然后利用该漏洞在用户的设备上执行恶意代码，这种攻击手段还比较容易识别。或者，攻击者会利用基于 Lhasa 库的文件扫描系统来读取 LZH 和 LHA 文件的内容，在这种情况下，攻击活动就更加隐蔽。一般情况下，当用户需要扫描不太常用的文件格式时，通常会依赖于能够扫描外来邮件附件以及互联网下载文件等内容的系统。这类扫描系统往往使用标准开源库来解析和提取这些文件的内容。但是，因为打开和扫描这些格式文件的不需要用户操作，所以恶意攻击者就有机会利用人们的这一常见盲点远程执行恶意代码。类似这样的漏洞有可能会被作为绕过安全控制措施非法访问组织系统的手段。

用户不应忽视因为该漏洞而遭到漏洞攻击的可能性（例如前面提到的通过第三方系统中包含的易受攻击的库发起的攻击）。

Snort 规则：37493、37494
ClamAV：BC.Unix.Exploit.Agent
FireAMP：Unix.Exploit.Agent

产品	保护
AMP	✔
CWS	✔
ESA	✔
网络安全	✔
WSA	✔

如需获取有关最新规则的信息，请参阅防御中心、FireSIGHT 管理中心或 Snort.org。鉴于此漏洞的性质，Web 和电子邮件保护目前由 AMP 提供。

发布者：MARTIN LEE；发布时间：下午 12:10
标签：CVE-2016-2347、漏洞、漏洞聚焦