



## Google's 新 Chrome 浏览器安全概览

2008 年 9 月 19 日



## 目录

概述.....	3
体系架构.....	3
对已知漏洞的描述.....	4
iSIGHT Partners 发现的原始漏洞.....	4
结论.....	4

## 概述

SaaS（软件即服务）在全球方兴未艾，谷歌的新 Chrome 浏览器应时而出并将会在 SaaS 的潮流中受益匪浅，尽管还在测试版阶段，谷歌浏览器显示其独特的页/进程的分离模式。iSIGHT Partner 实验室对其已经有了一个简要的研究。

## 体系架构

Google Chrome 浏览器发行版源代码由存储在 1400 个文件夹下的近 30000 个文件组成。其中大部分文件为测试浏览器功能与操作模块的数据文件，包含在 240 个位置超过 4200 个文件。这些文件分为以下主要类别：

大约有 15-20%的文件在发行版中标记为第三方文件，用于建立和测试 Chrome。第三方文件包括：

- | Lighttpd web 服务；
- | Cygwin, windows 下的类 Unix 环境；
- | Python, 脚本编程语言；
- | Zlib 库, 用于 deflate 压缩方法；
- | Libpng 库, 用于处理 PNG 格式图片。

源代码发行版中，大多数这种类别的文件被用于测试和建立 Chrome。通过包括二进制文件的工具，编译后的 Chrome 被相应地缩小了，因为工具的依赖并不需要认证。

同时二进制发行版格式是“Google Gears”插件，一种网络应用程序，允许建立和执行桌面 web 应用程序。

Chrome 使用 WebKit 开源浏览器引擎解释 HTML 内容，该引擎也应用于 Apple 的 Safari 浏览器和 Adobe AIR 运行环境。Chrome 使用的 WebKit 版本是 525.13，该版本也用于 Safari 3.1，Safari 最新版本 3.1.2 采用 WebKit 525.19 引擎。

Chrome 与其它比较流行的浏览器的最大区别是浏览器标签的进程分离。与其它浏览器不同的是，每个标签运行于自身的内存空间，且关闭一个标签也关闭进程并释放分配的内存。这个功能的设计改进了内存管理和提高应用程序的稳定性。Chrome 浏览器本身作为各标签子进程的父进程运行，每个子进程“沙箱”，只能与外部世界的通过有限 API 沟通，这是用来发送信息之间的父进程和子进程。允许此功能的代码位于“sandbox/”子目录。

由于子进程只能得到有限的系统资源，子进程必须向父进程确认功能请求，而且父进程最终决定是否为

子进程提供额外功能或资源。该行为是允许在应用层面强制执行一些低级别的功能覆盖。正因为如此，一个沙盒中的进程不能直接访问某些系统级资源。

一个明显的例外是上述网络协议，它的运行不受父进程的限制。这一例外提高了性能，但它同时提供了一个重要的攻击层面；与其它浏览器一样，网络中的任何代码的脆弱性往往被视为被利用的或危险的。

## 对已知漏洞的描述

已经有一些 Chrome 的重要漏洞的报道。这些漏洞与 Apple Safari 之前版本的漏洞很相似，而且都被认为是由旧版本的 WebKit 库所产生的。iSIGHT Partners 测试了这些漏洞，结果很相近。然而，报告的其他 Safari 浏览器的漏洞可能不会影响 Chrome，因为 Chrome 使用（默认编译器设置）谷歌的 V8 JavaScript 引擎，它是一个开放源码的引擎。由于这一变化，一些以前报告的影响 Safari 浏览器中 WebKit 组件的弱点，对 V8 引擎将不再有影响，虽然这不应该被用来断定 V8 引擎比默认 WebKit 的引擎有多么安全。

## iSIGHT Partners 发现的原始漏洞

同时，iSIGHT Partners 实验室已经发现了 Chrome 在处理带有“Transfer - encoding”类型块的 HTTP 流量的时候存在一个漏洞。通过提供一个负的长度，有可能导致堆的内容由控制量转移。虽然线程导致堆修改会崩溃，并引发其他代码的执行（最终导致进程被终止），其他使用同一个堆的线程会在应用程序退出之前访问该堆。通过掌控攻击事件发生的时间，在特定的时刻，以特定的顺序，向 Chrome 浏览器发送攻击数据，远程攻击者可以使应用程序访问堆的数据，并执行任意代码。虽然这种性质的攻击的可靠性不是很高，代码执行可能没有访问一个恶意网站那样容易。此外，由于 Chrome 浏览器对过程的处理方式，即使应用程序运行很长时间，它的状态还是非常容易识别的，所以它被利用的可能性会更高。iSIGHT Partners 将继续关注这个问题，并随时报告最新的进展。

## 结论

谷歌 Chrome 浏览器，虽然它目前只是 Beta 版本，但有几个原因可能使它继续被大家关注。首先，它是谷歌产品，众所周知，谷歌延长了软件的 beta 测试阶段，以企图逃脱其责任。谷歌的这一测试阶段，并不妨碍其市场渗透和开拓；谷歌桌面搜索引擎处于测试版很多年了，但每天仍然被成千上万的用户所采用。由于计算机世界中 web 的趋势是必然的，同时谷歌的拥有卓越的技术和信誉，我们可以猜想那些早期使用 Chrome 浏览器的用户可能并没有意识到存在的安全问题。