HTTPOXY -- CGI 环境变量劫持漏洞分析

云破 / 2016-10-19 08:51:06 / 浏览数 24011 安全技术 漏洞分析 顶(0) 踩(0)

0x00 前言

 7月18日，一个名为 HTTPOXY 的漏洞在安全圈内广泛传播。云盾攻防对抗团队第一时间对此漏洞进行了深入分析，发现其本质是一个 CGI 环境变量劫持漏洞，对 CGI 的环境变量 HTTP_PROXY 变量进行劫持。如果 CGI 在运行过程中依赖 HTTP_PROXY，那么攻击者将能够获取到程序敏感数据，甚至伪造返回包对 CGI 程序实现欺骗。

0x01 漏洞分析

 这个漏洞实际上 CGI 程序对变量命名不规范导致的。CGI 程序在接收到 HTTP Header 后，会把部分 Header 的信息存入以 HTTP_ 开头的变量中。Header 中要是出现了 Proxy 头，那么 Proxy 头中的信息会存放在 HTTP_PROXY 的变量中。巧合的是，CGI 程序环境变量中本身就定义了一个 HTTP_PROXY 变量，作用是为 CGI 程序设置代理。因此，如果我们在请求中带上了 Proxy 头，那么 HTTP_PROXY 变量将会被我们发送的内容覆盖，实现 HTTP_PROXY 变量劫持。需要注意的是，覆盖的变量只对当次请求有效，不会对全局的 HTTP_PROXY 变量造成影响。
 我们在 x.x.27.216 上用 nc 监听 23333 端口，然后向受害网站 x.x.25.84 发送的请求中加入 Proxy 头 "x.x.27.216:23333"。如下图所示，受害网站在向 restapi.amap.com 请求数据，而这个请求被我们的机器截获到了，漏洞利用成功。同时，这个请求将网站在 restapi.amap.com 使用的 KEY 暴露出来了，造成敏感信息泄漏。

 这里分享一下我们想到的两个利用场景：
 1、CGI 程序与其它网站通信时，需要 CGI 程序带上某些身份信息的，如 AccessToken、gsid、key 等，那么这些敏感信息将会被非法的代理服务器接收到，造成敏感信息泄漏。
 2、对于电商类网站，若通过设置 Proxy 头能截获到它向支付网关发送的请求，那么就可以篡改这个请求的返回包，如“将支付失败改为支付成功”，对原网站进行欺骗。

0x02 影响范围

 理论上这个漏洞影响所有以 CGI 方式运行的程序。但漏洞利用受到以下限制：
 1、CGI 程序不会对外发送请求；
 2、CGI 程序不依赖 HTTP_PROXY 变量；
 3、CGI 程序与外部使用非 HTTP 协议（如 HTTPS）进行通信。
 如果符合上述其中一种情况，漏洞将无法利用。我们认为，此漏洞的危害程度没有外界宣传的那么高。

0x03 修复方案

 Proxy 并非一个规范的 HTTP Header，因此我们没必要去处理 HTTP 请求中 Proxy 头的内容。 由于每个应用的修复方案不一样，下面以 Nginx 和 Apache 进行举例：
 Nginx：在调用 FastCGI 的地方将 HTTP_PROXY 置为空。

```
fastcgi_param HTTP_PROXY "";
```

Apache：借助 mod_headers 模块将 Proxy 头置为失效。

```
RequestHeader unset Proxy early
```

其它应用的修复方案请参考应用官方公告或 0x04 中的参考资料。

0x04 参考资料

0: https://httpoxy.org/

1: http://www.iana.org/assignments/message-headers/message-headers.xhtml

2: https://access.redhat.com/security/vulnerabilities/httpoxy

上一篇：道哥为你讲解漏洞披露的前世今生 下一篇：《中国互联网地下产业链分析白皮书》

1. 1 条回复

男仔无才 2016-10-19 09:26:53

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板