Moxa Command Injection / Cross Site Scripting / Vulnerable Software

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

Posted Sep 1, 2021

Many Moxa devices suffer from command injection, cross site scripting, and outdated software vulnerabilities.

tags | exploit, vulnerability, xss
advisories | CVE-2013-1914, CVE-2013-7423, CVE-2015-0235, CVE-2015-7547, CVE-2016-1234, CVE-2021-39278, CVE-2021-39279
SHA-256 | 91e5218cfa2c2452c1da0918b3b85328aad5bcf76352c949affc7a9a10a95a39 Download | Favorite | View

Related Files

Change Mirror Download

```
SEC Consult Vulnerability Lab Security Advisory < 20210901-0 >
=======================================================================
             title: Multiple vulnerabilities
           product: see "Vulnerable / tested versions"
  vulnerable version: see "Vulnerable / tested versions"
       fixed version: see "Solution"
          CVE number: CVE-2021-39278, CVE-2021-39279
              impact: High
            homepage: https://www.moxa.com/
               found: 2020-08-31
                  by: 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:
-------------------
"Together, We Create Change

Moxa is committed to making a positive impact around the world. We put our all
behind this commitment--from our employees, to our products and supply chain.

In our local communities, we nurture and support the spirit of volunteering.
We encourage our employees to contribute to community development, with an
emphasis on ecology, education, and health.

In our products, we invest in social awareness programs and
environment-friendly policies at every stage of the product lifecycle. We make
sure our manufacturing meets the highest standards with regards to quality,
ethics, and sustainability."

Source: https://www.moxa.com/en/about-us/corporate-responsibility

Business recommendation:
------------------------
SEC Consult recommends to immediately apply the available patches
from the vendor. A thorough security review should be performed by
security professionals to identify further potential security issues.


Vulnerability overview/description:
-----------------------------------
1) Authenticated Command Injection (CVE-2021-39279)
An authenticated command injection vulnerability can be triggered by issuing a
GET request to the "/forms/web_importTFTP" CGI program which is available on
the web interface. An attacker can abuse this vulnerability to compromise the
operating system of the device. This issue was found by emulating the firmware
of the device.

2) Reflected Cross-Site Scripting via Manipulated Config-File (CVE-2021-39278)
Via a crafted config-file, a reflected cross-site scripting vulnerability can
be exploited in the context of the victim's browser. This config-file can be
uploaded to the device via the "Config Import Export" tab in the main menu.

3) Known GNU glibc Vulnerabilities (CVE-2015-0235)
The used GNU glibc in version 2.9 is outdated and contains multiple known
vulnerabilities. One of the discovered vulnerabilities (CVE-2015-0235,
gethostbyname "GHOST" buffer overflow) was verified by using the MEDUSA
scalable firmware runtime.

4) Multiple Outdated Software Components
Multiple outdated software components containing vulnerabilities were found by
the IoT Inspector.

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

Proof of concept:
-----------------
1) Authenticated Command Injection (CVE-2021-39279)
The vulnerability can be triggered by navigating in the web interface to the
tab:

"Main Menu"->"Maintenance"->"Config Import Export"

The "TFTP Import" menu is prone to command injection via all parameters. To
exploit the vulnerability, an IP address, a configuration path and a filename
must be set.
If the filename is used to trigger the exploit, the payload in the interceptor
proxy would be:

http://192.168.1.1/forms/web_importTFTP?servIP=192.168.1.1&configPath=/&fileName=name|`ping localhost -c 100`


2) Reflected Cross-Site Scripting via Manipulated Config-File (CVE-2021-39278)
The vulnerability can be triggered by navigating in the web interface to the
tab:

"Main Menu"->"Maintenance"->"Config Import Export"

The "Config Import" menu is prone to reflected cross-site scripting via the
upload of config files. Example of malicious config file:
-------------------------------------------------------------------------------
[board]
deviceName="WAC-2004_0000</span><script>alert(document.cookie)</script>"
deviceLocation=""
[..]
-------------------------------------------------------------------------------
Uploading such a crafted file triggers cross-site scripting as the erroneous
value is displayed without filtering characters.


3) Known GNU glibc Vulnerabilities (CVE-2015-0235)
GNU glibc version 2.9 contains multiple CVEs like:
CVE-2016-1234, CVE-2015-7547, CVE-2013-7423, CVE-2013-1914, and more.

The gethostbyname buffer overflow vulnerability (GHOST) was checked with the
help of the exploit code from https://seclists.org/oss-sec/2015/q1/274. It was
compiled and executed on the emulated device to test the system.


4) Multiple Outdated Software Components
The IoT Inspector recognized multiple outdated software components with known
vulnerabilities:

BusyBox         1.18.5    06/2011
```


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 157 files
- Ubuntu 76 files
- LiquidWorm 23 files
- Debian 21 files
- nu11secur1ty 11 files
- malvuln 11 files
- Gentoo 9 files
- Google Security Research 8 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)

```
Dropbear SSH    2011.54  11/2011
GNU glibc       2.9      02/2009
Linux Kernel    2.6.27   10/2008
OpenSSL         0.9.7g   04/2005
Only found in the program "iw_director"
OpenSSL         1.0.0    03/2010


Vulnerable / tested versions:
-----------------------------
The following firmware versions for various devices have been identified
to be vulnerable:
* WAC-2004               / 1.7
* WAC-1001               / 2.1
* WAC-1001-T             / 2.1
* OnCell G3470A-LTE-EU   / 1.7
* OnCell G3470A-LTE-EU-T / 1.7
* TAP-323-EU-CT-T        / 1.3
* TAP-323-US-CT-T        / 1.3
* TAP-323-JP-CT-T        / 1.3
* WDR-3124A-EU           / 2.3
* WDR-3124A-EU-T         / 2.3
* WDR-3124A-US           / 2.3
* WDR-3124A-US-T         / 2.3


Vendor contact timeline:
------------------------
2020-10-09: Contacting vendor through moxa.csrt@moxa.com.
2020-10-12: Contact sends PGP key for encrypted communication and asks for the
            detailed advisory. Sent encrypted advisory to vendor.
2020-11-06: Status update from vendor regarding technical analysis. Vendor
            requested more time for fixing the vulnerabilities as more products
            are affected.
2020-11-09: Granted more time for fixing to vendor.
2020-11-10: Vendor asked for next steps regarding the advisory publication.
2020-11-11: Asked vendor for an estimation when a public disclosure is possible.
2020-11-16: Vendor responded that the product team can give a rough feedback.
2020-11-25: Asked for a status update.
2020-11-25: Vendor responded that the investigation is not done yet.
2020-12-14: Vendor provided a list of potential affected devices and stated
            that full investigation may take until January 2021 due to the list
            of CVEs that were provided with the appended IoT Inspector report.
            The patches may be available until June 2021.
2020-12-15: Shifted next status update round with vendor on May 2021.
2020-12-23: Vendor provided full list of affected devices.
2021-02-05: Vendor sieved out the found issues from 4) manually and provided a
            full list of confirmed vulnerabilities. WAC-2004 phased-out in
            2019.
2021-02-21: Confirmed receive of vulnerabilities, next status update in May
            2021.
2021-06-10: Asking for an update.
2021-06-15: Vendor stated, that the update will be provided in the next days.
2021-06-21: Vendor will give an update in the next week as Covid gets worse in
            Taiwan.
2021-06-23: Vendor stated, that patches are under development. Vendor needs more
            time to finish the patches.
2021-06-24: Set release date to 2021-09-01.
2021-07-02: Vendor provides status updates.
2021-08-16: Vendor provides status updates.
2021-08-17: Vendor asks for CVE IDs and stated, that WDR-3124A has phased-out.
2021-08-20: Sent assigned CVE-IDs to vendor. Asked for fixed version numbers.
2021-08-31: Vendor provides fixed firmware version numbers and the advisory
            links.
2021-09-01: Coordinated release of security advisory.

Solution:
---------
According to the vendor the following patches must be applied to fix issues:
* WAC-1001               / 2.1.5
* WAC-1001-T             / 2.1.5
* OnCell G3470A-LTE-EU   / 1.7.4
* OnCell G3470A-LTE-EU-T / 1.7.4
* TAP-323-EU-CT-T        / 1.8.1
* TAP-323-US-CT-T        / 1.8.1
* TAP-323-JP-CT-T        / 1.8.1

The Moxa Technical Support must be contacted for requesting the security
patches.

The corresponding security advisories for the affected devices are available on
the vendor's website:
TAP-323/WAC-1001/WAC-2004
https://www.moxa.com/en/support/product-support/security-advisory/tap-323-wac-1001-2004-wireless-ap-bridge-
client-vulnerabilities
OnCell G3470A-LTE/WDR-3124A
https://www.moxa.com/en/support/product-support/security-advisory/oncell-g3470a-wdr-3124a-cellular-gateways-
router-vulnerabilities

The following device models are EOL and should be replaced:
* WAC-2004
* WDR-3124A-EU
* WDR-3124A-EU-T
* WDR-3124A-US
* WDR-3124A-US-T


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

EOF Thomas Weber / @2021
```


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

Site Links
News by Month
News Tags
Files by Month
File Tags

About Us
History & Purpose
Contact Information
Terms of Service
Privacy Statement

Hosting By
Rokasec

Follow us on Twitter
Subscribe to an RSS Feed

File Directory Copyright Information