

New issue

[Jump to bottom](#)

Stored XSS when updating analysis details #375

🔒 Closed

lum8rjack opened this issue on Mar 29, 2020 · 3 comments

lum8rjack commented on Mar 29, 2020

The application does not sanitize the user input when updating the details of a firmware. When updating the firmware details, the applications posts the data to the "upload-analysis/[uid]" page. That page then runs the function "_get_meta_from_request()" within the /src/helperFunctions/mongo_task_conversion.py script. I tested the "tags" and "version" fields by adding JavaScript to the updated fields (it looks like other fields are possibly vulnerable too). This data is not sanitized and is stored in the application. Each time a page is requested with this information, the JavaScript is ran. I added some screenshots to help. Using the "escape" function within flask could be a solution to sanitize the input. I tested it against the version field and it worked. Let me know if there are any additional questions.

Filter: Hiding out of scope items: hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies
48	http://192.168.1.8:5000	POST	/update-analysis/ae35e2773a2c9d7de7b405df385fbc286b1a65669297662af3b890dd9ac7858e_1201163			200	9540	HTML		FACT			192.168.1.8	session=eyJ2rj...
49	http://192.168.1.8:5000	GET	/analysis/ae35e2773a2c9d7de7b405df385fbc286b1a65669297662af3b890dd9ac7858e_1201163			200	38862	HTML		FACT			192.168.1.8	session=eyJ2rj...
50	http://192.168.1.8:5000	GET	/static/js/tree/jquery.min.js			304	350	script	js				192.168.1.8	session=eyJ2rj...
51	http://192.168.1.8:5000	GET	/static/js/tree/jquery.min.js			304	348	script	js				192.168.1.8	session=eyJ2rj...

Request Response

Raw Params Headers Hex

```
37
38
39 .....-20589733272407758006623354261
40 Content-Disposition: form-data; name="device_part_dropwen"
41
42 .....-20589733272407758006623354261
44 Content-Disposition: form-data; name="device_part"
45
46 .....-20589733272407758006623354261
48 Content-Disposition: form-data; name="version"
49
50 5.03.20
51 .....-20589733272407758006623354261
52 Content-Disposition: form-data; name="release_date"
53
54 1070-Q1-Q3
55 .....-20589733272407758006623354261
56 Content-Disposition: form-data; name="tags"
57
58 router, belkinscript>alert(1)</script>
59 .....-20589733272407758006623354261
60 Content-Disposition: form-data; name="analysis_systems"
61
62 crypts_material
63 .....-20589733272407758006623354261
64 Content-Disposition: form-data; name="analysis_systems"
65
66 ip_and_uri_finder
67 .....-20589733272407758006623354261
68 Content-Disposition: form-data; name="analysis_systems"
69
70 printable_strings
71 .....-20589733272407758006623354261
72 Content-Disposition: form-data; name="file_name"
73
74 FRK1002_MU_5_03.20.bin
75 .....-20589733272407758006623354261
76
```

Adding js to the tags field

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Logging of out-of-scope Proxy traffic is disabled Re-enable

Filter: Hiding out of scope items: hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title
58	http://192.168.1.8:5000	GET	/			200	21985	HTML		FA
60	http://192.168.1.8:5000	GET	/static/bootstrap/js/bootstrap-datetimepicker.min.js			304	355	script	js	
63	http://192.168.1.8:5000	GET	/static/bootstrap/js/jquery.min.js			304	349	script	js	

Request Response

Raw Headers Hex HTML Render

```
276 Wyze WyzeCamv2 - 4.9.5.36 (Camera)
277 <span class=label label-pill label-info pull-right" style="font-size: 10px;">Uboot</span>
278 <span class=label label-pill label-default pull-right" style="font-size: 10px;"><cam/>span>
279 <span class=label label-pill label-default pull-right" style="font-size: 10px;">firmware</span>
280 <span class=label label-pill label-default pull-right" style="font-size: 10px;">wyze</span>
281
282 </div>
283 </a>
284 <div><font face="courier" style="font-size: 12px;">50b9282b37ef1d67ec61e3c3f51437e5227c72c9bc7cb6c232df733d81954ef5_11075648</font>
285 <a href="/download/50b9282b37ef1d67ec61e3c3f51437e5227c72c9bc7cb6c232df733d81954ef5_11075648" class="glyphicon glyphicon-download-alt pull-right"></a>
286 </div>
287 </td>
288 </tr>
289
290 <tr>
291 <td class="active"> 2020-03-20 11:39:40 </td>
292 <td class="active clickable" onclick="location.href='/analysis/ae35e2773a2c9d7de7b405df385fbc286b1a65669297662af3b890dd9ac7858e_1201163'">
293 <a href="/analysis/ae35e2773a2c9d7de7b405df385fbc286b1a65669297662af3b890dd9ac7858e_1201163" style="color: rgb(51, 51, 51);">
294 <div style="width: 100%; height: 100%;">
295 Belkin N300 - 5.03.20 (Router)
296 <span class=label label-pill label-default pull-right" style="font-size: 10px;">belkin<script>alert(1)</script></span>
297 <span class=label label-pill label-info pull-right" style="font-size: 10px;">generic_carver</span>
298 <span class=label label-pill label-default pull-right" style="font-size: 10px;">router</span>
299
300 </div>
```

When browsing to the home page it loads the js

FACT

192.168.1.8:5000

FACT Firmware Analysis and Comparison Tool

Home Database Upload Info

General Facts

firmware samples	0
firmware total size	246.27 MiB
firmware average size	30.78 MiB
unique included files	4,110
unique included files total size	
unique included files average size	
statistic generation time	

Latest Submissions

Showing 8 out of 8 firmwares in the database.

Submission Time	Firmware
2020-03-28 12:35:38	Netgear Nighthawk R8000 - 1.0.4.46_30.1.63 (Router) 4795d83b875d9bcead17a38a439ea24d72778bc32cb2e8f1Bd85d8fa0ee_30433338
2020-03-23 21:24:05	SiliconDust HDHomeRun Extend - 20200225 (Antenna Tuner) 98034cc312a24459388304490f9c88778842e91a54e0950aa57ac0506b167d_3455376
	Wyze WyzeCamv2 - 4.9.5.36 (Camera) 50b9282b37ef1d67ec61e3c3f51437e5227c72c9bc7cb6c232df733d81954ef5_11075648
	Belkin N300 - 5.03.20 (Router)

1

OK

js is executed

```

iot@ubuntu16: ~/FACT_core/src/helperFunctions
import logging
import os
import re
import sys
from tempfile import TemporaryDirectory

#ADDED
from flask import escape

from helperFunctions.uid import create_uid
from objects.firmware import Firmware

OPTIONAL_FIELDS = ['tags', 'device_part']
DROPDOWN_FIELDS = ['device_class', 'vendor', 'device_name', 'device_part']

def create_analysis_task(request):
    task = _get_meta_from_request(request)
    if request.files['file']:
        task['file_name'], task['binary'] = get_file_name_and_binary_from_request(request)
        task['uid'] = get_uid_of_analysis_task(task)
    if task['release_date'] == '':
        # set default value if date field is empty
        task['release_date'] = '1970-01-01'
    return task


def get_file_name_and_binary_from_request(request): # pylint: disable=invalid-name
    try:
        file_name = request.files['file'].filename
    except Exception:
        file_name = 'no_name'
    file_binary = get_uploaded_file_binary(request.files['file'])
    return file_name, file_binary

def create_re_analyze_task(request, uid):
    task = _get_meta_from_request(request)
    task['uid'] = uid
    if not task['release_date']:
        task['release_date'] = '1970-01-01'
    return task

def _get_meta_from_request(request):
    meta = {
        'device_name': request.form['device_name'],
        'device_part': request.form['device_part'],
        'device_class': request.form['device_class'],
        'vendor': request.form['vendor'],
        #ADDED escape function
        'version': escape(request.form['version']),
        'release_date': request.form['release_date'],
        'requested_analysis_systems': request.form.getlist('analysis_systems'),
    }
    "mongo_task_conversion.py" 137L, 4398C

```

Used the escape function to sanitize the input


Firmware Analysis and Comparison Tool

[Home](#)
[Database](#)
[Upload](#)
[Info](#)

Analysis for Belkin N300 v. 5.03.20<script>alert(1)</script>

UID: ae35e2773a2c9d7de7b405df385fbc286b1a65669297662af3b890dd9ac7858e_1201163

General		Analysis Results
device name	N300	crypto material
vendor	Belkin	file hashes
device class	Router	file type
version	5.03.20<script>alert(1)</script>	ip and uri finder
release date	unknown	printable strings
file name	F9K1002_WW_5.03.20.bin	unpacker
virtual path	<ul style="list-style-type: none"> Belkin N300 - 5.03.20<script>alert(1)</script> (Router) 	Run additional analysis
file size	1.15 MiB (1,201,163 bytes)	
Tags	belkin router	
file type	data	

File Tree

dorpvom commented on Mar 30, 2020

Collaborator

Hi,

we actually did not do a great job securing our web application, thus the warning in our *readme*. That said we're happy to improve security wherever possible. Mostly we simply lack the background in web application design.

Would you like to open a Pull Request on that yourself, since you seem to have a solution already?

Best,
Johannes

lum8rjack commented on Mar 30, 2020

Author

Thanks for the quick response. Yeah I can test the solution to make sure it works and doesn't affect anything else and then open a pull request.

Clint



lum8rjack mentioned this issue on Mar 30, 2020

Fix XSS bug by escaping user input when updating firmware details #376

Merged

weidenba commented on Mar 31, 2020

Contributor

fix merged



weidenba closed this as completed on Mar 31, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants

