[SYSS-2020-030]: Jira module "Gantt-Chart for Jira" - Cross-Site Scripting (CWE-79) (CVE-2020-15944)

From: Sebastian Auwärter <sebastian.auwaerter () syss de>
Date: Mon, 3 Aug 2020 16:58:02 +0200

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

Advisory ID: SYSS-2020-030
Product: Jira module "Gantt-Chart for Jira"
Manufacturer: Frank Polscheit - Solutions & IT-Consulting
Affected Version(s): <=5.5.4
Tested Version(s): 5.5.3, 5.5.4
Vulnerability Type: Cross-Site Scripting (CWE-79)
Risk Level: Medium
Solution Status: Fixed
Manufacturer Notification: 2020-07-23
Solution Date: 2020-07-31
Public Disclosure: 2020-08-03
CVE Reference: CVE-2020-15944
Author of Advisory: Sebastian Auwaerter, SySS GmbH

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Overview:

Gantt-Chart for Jira is a Jira module for displaying Gantt charts.

The manufacturer describes the product as follows (see [1]):

"High performance Gantt-Chart capable to display multi-projects with
10.000+ issues aggregating them as top-level big picture"

Due to missing validation of user input, the module is vulnerable to
a persistent cross-site scripting attack. As described in
security advisory SYSS-2020-029 (see [4]), it is also possible to
attack other users with this attack vector.

To exploit this vulnerability, an attacker has to be authenticated.

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Vulnerability Details:

The vulnerability exists because the names of newly created filters
are not properly sanitized by the extension. A simple attack vector
like "<script>alert('XSS')</script>" can be chosen as the name of
a filter and is then displayed on every load of the vulnerable module.

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Proof of Concept (PoC):

This security vulnerability can be reproduced by simply creating a new
filter with the "filter name" "<script>alert('XSS')</script>". Whenever
the dashboard with the vulnerable module is loaded, the attack vector
gets executed.

The following request is sent to the web server:

PUT /rest/gantt/1.0/user/properties/<chart_id>?userKey=<your_user_name>
HTTP/1.1
Host: <victim_host>
[...]

[...]"filters":{{"search":""},"<script>alert(\"XSS\")</script>"}[...]

!!! This filter can not be easily removed via the web interface. !!!
!!!                    Use with caution.                         !!!

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Solution:

Update to software version 5.5.5

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Disclosure Timeline:

2020-07-21: Vulnerability discovered
2020-07-23: Vulnerability reported to manufacturer
2020-07-31: Patch released by manufacturer
2020-08-03: Public disclosure of vulnerability

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

References:

[1] Product Website for Jira Module "Gantt-Chart"

https://marketplace.atlassian.com/apps/28997/gantt-chart-for-jira?hosting=cloud&tab=overview
[2] SySS Security Advisory SYSS-2020-030

https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2020-030.txt
[3] SySS Responsible Disclosure Policy
    https://www.syss.de/en/news/responsible-disclosure-policy/
[4] SySS Security Advisory SYSS-2020-029

https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2020-029.txt

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Credits:

This security vulnerability was found by Sebastian Auwaerter of SySS
GmbH.

E-Mail: sebastian.auwaerter () syss de
Public Key:
https://www.syss.de/fileadmin/dokumente/PGPKeys/Sebastian_Auwaerter.asc
Key Fingerprint: F98C 3E12 6713 19D9 9E2F BE3E E9A3 0D48 E2F0 A8B6

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Disclaimer:
```

```
The information provided in this security advisory is provided "as is"
and without warranty of any kind. Details of this security advisory may
be updated in order to provide as accurate information as possible. The
latest version of this security advisory is available on the SySS website.
-----BEGIN PGP SIGNATURE-----

iQIzBAEBCgAdFiEE+Yw+EmcTGdmeL74+6aMNSOLwqLYFAl8oFcIACgkQ6aMNSOLw
qLbWlQ//Z8n259oL2XArwBpHhv7Le8MEbPmE255MtUSr4JUsNus3Rrsie5zJE9Hb
Sqfom7a/CPgjKJslWiaKH0D6UmUWX8nPY2wEE9FtTdNQ/E48QiqtgD4XFA5oUBTx
pawGADuia9NY4wYcTofe5IJBMci+jhxJDQv394zywhRzg3OTiB8UdPYBGbCJnywO
O8xV5vwkw+8LuQAVdFbjpZMrjT8C/yuC2MrOCt+gtV4eF7isMaMarTwZjQFX4wNY
3twritwL/wQPvsftTfpZ9dWX3lqaRA9pLBZPsyQilHU4Pp4O4zMB4j+aH5gqmIGF
B+m6m9hZVE/3Sz5OspXUfShnUwRkFWRob7Xzbl7s+nWMitN+/2P3MAlus6JBbPgj
5/HPwlthXrlXcY/mu4M9Aan9pay+gKArRIQ82gI2Zbe5S8yp+2NhWNH64Nl3dKSm
L5JHflvh8veGDCOSuzYdoU2GJywhFQ4aMMuhnleA8zJBSBdFmUbyelXFrUEE4KZ8
0E5N3Fg3vbvdYpp+Ow+X+t5vj7gZcpURn3OwY78oR3nKICWASDjDG+WT5oAcjl6R
arDE2MEffya4EP70fOhhwDM3SjvgiwlCXDKRLHavZ+bWNHpbLLu3swWHD5kUpMlX
Qx1STPwGf0bUEsiE8mmhHx+wl7q/O+hAgoU9Fw2cQObAkxJ4ilQ=
=5Gtt
-----END PGP SIGNATURE-----
```

By Date By Thread

Current thread:

[SYSS-2020-030]: Jira module "Gantt-Chart for Jira" - Cross-Site Scripting (CWE-79)(CVE-2020-15944) ***Sebastian Auwärter (Aug 04)***