

Gantt-Chart For Jira 5.5.4 Cross Site Scripting

Authored by [Sebastian Auwaerter](#) | Site [sysS.de](#)

Posted Aug 4, 2020

Gantt-Chart for Jira versions 5.5.4 and below suffer from a cross site scripting vulnerability.

tags | [exploit](#), [xss](#)

advisories | [CVE-2020-15944](#)

SHA-256 | dba9c39f62d06702328bfd60b00d5294682d93fffb3a9a32da2fcec3d90878c [Download](#) | [Favorite](#) | [View](#)

Related Files

Share This

Like

Twitter

LinkedIn

Reddit

Digg

StumbleUpon

Change Mirror

Download

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

Advisory ID: SYSS-2020-030
Product: Jira module "Gantt-Chart for Jira"
Manufacturer: Frank Polschelt - 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+YwEmcTGDmeL74+6aMNSOLwqLFFA18FcIACgKq6aMNSOLw
qLW1QI/2BaZ5oL2XaWqgJhV7LeSHBzPzE25MkU8r4JUsNus3Krsle5aJE79Hb
SgFom7a/CPgJKJslWiaKH0D6U6mXK8nPV2wEE9FTDnQ/E48QlqtGD4XFA5oSBTz
pawGAUia9NtY4VcToFe5IJBMcI+jhkJDQv394zyvhrz30T18RdUPYBgBCJny0Y
08xV5vkwk+8LuQAVdFbjpZMrjT8C/yuC2MrOCT+gtV4eF7IaMaMaTW2jQPF4wNY
```

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr
Sa					
				1	2
3					
4	5	6	7	8	9
10					
11	12	13	14	15	16
17					
18	19	20	21	22	23
24					
25	26	27	28	29	30
31					

Top Authors In Last 30 Days

Red Hat 150 files
Ubuntu 68 files
LiquidWorm 23 files
Debian 16 files
malvuln 11 files
nu11security 11 files
Gentoo 9 files
Google Security Research 6 files
Julien Ahrens 4 files
T. Weber 4 files

File Tags

ActiveX (932)	December 2022
Advisory (79,754)	November 2022
Arbitrary (15,694)	October 2022
BBS (2,859)	September 2022
Bypass (1,619)	August 2022
CGI (1,018)	July 2022
Code Execution (8,926)	June 2022
Conference (673)	May 2022
Cracker (840)	April 2022
CSRF (3,290)	March 2022
DoS (22,602)	February 2022
Encryption (2,349)	January 2022
Exploit (50,359)	Older

File Inclusion (4,165)

File Upload (946)

Firewall (821)

Info Disclosure (2,660)

Intrusion Detection (867)

Java (2,899)

JavaScript (821)

Kernel (6,291)

Local (14,201)

Magazine (586)

Overflow (12,419)

Perl (1,418)

PHP (5,093)

Proof of Concept (2,291)

Protocol (3,435)

Python (1,467)

Remote (30,044)

Root (3,504)

Ruby (594)

Scanner (1,631)

Security Tool (7,777)

Shell (3,103)

Shellcode (1,204)

Sniffer (886)

File Archives

December 2022

November 2022

October 2022

September 2022

August 2022

July 2022

June 2022

May 2022

April 2022

March 2022

February 2022

January 2022

Older

Systems

AIX (426)

Apple (1,926)

BSD (370)

CentOS (55)

Cisco (1,917)

Debian (6,634)

Fedora (1,600)

FreeBSD (1,242)

Gentoo (4,272)

HPUX (878)

IOS (330)

iPhone (108)

IRIX (220)

Juniper (67)

Linux (44,315)

Mac OS X (684)

Mandriva (3,105)

NetBSD (255)

OpenBSD (479)

RedHat (12,469)

Slackware (941)

Solaris (1,607)

```
3twritwL/wQPvfeftTfp29dXK1qaRA9pLB2PayQl1HU4Pp404zMB4j+uH5gqmIGF
B+m6m9hZVE/3S250apXUfShnDwRkFWRcb7Xzb17a+nMM1tN+/2P3MA1us6JDBPgj
5/HpW1thXr1XcY/mu4M9Aan9pay+gKAzRIQ82gT2Zbe5S8yp+2NhWNH64N13dKSm
L5JHf1vh8veGDC08uzYdoU2GJywhFQ4aM9ubh1eA8zJB9BdFwUbye1XFrUEE4KZ2
GE5N3Pg3vbdvdlpp+QwX+5vj7g2cpURn30w78uR3nK1CWA5DJDG+WE5oAe-j16R
ar5E2MEffya4EP70fOhhwDM3Sjvq1w1CXDKRLHav2+bWNHpbLLu3awWED5kUpM1X
Qk1STPwGfObUEs1E8mmhix+w17g/O+hAgoU9Pw2cQObAkkJ4i1Q=
~5Gltt
-----END PGP SIGNATURE-----
```

[Login](#) or [Register](#) to add favorites

- [Spoof \(2,166\)](#)
- [SQL Injection \(16,102\)](#)
- [TCP \(2,379\)](#)
- [Trojan \(686\)](#)
- [UDP \(876\)](#)
- [Virus \(662\)](#)
- [Vulnerability \(31,136\)](#)
- [Web \(9,365\)](#)
- [Whitepaper \(3,729\)](#)
- [x86 \(946\)](#)
- [XSS \(17,494\)](#)
- [Other](#)
- [SUSE \(1,444\)](#)
- [Ubuntu \(8,199\)](#)
- [UNIX \(9,159\)](#)
- [UnixWare \(185\)](#)
- [Windows \(6,511\)](#)
- [Other](#)

Site Links


- [News by Month](#)
- [News Tags](#)
- [Files by Month](#)
- [File Tags](#)
- [File Directory](#)


About Us

- [History & Purpose](#)
- [Contact Information](#)
- [Terms of Service](#)
- [Privacy Statement](#)
- [Copyright Information](#)

Hosting By

- [Rokasec](#)

 Follow us on Twitter

 Subscribe to an RSS Feed