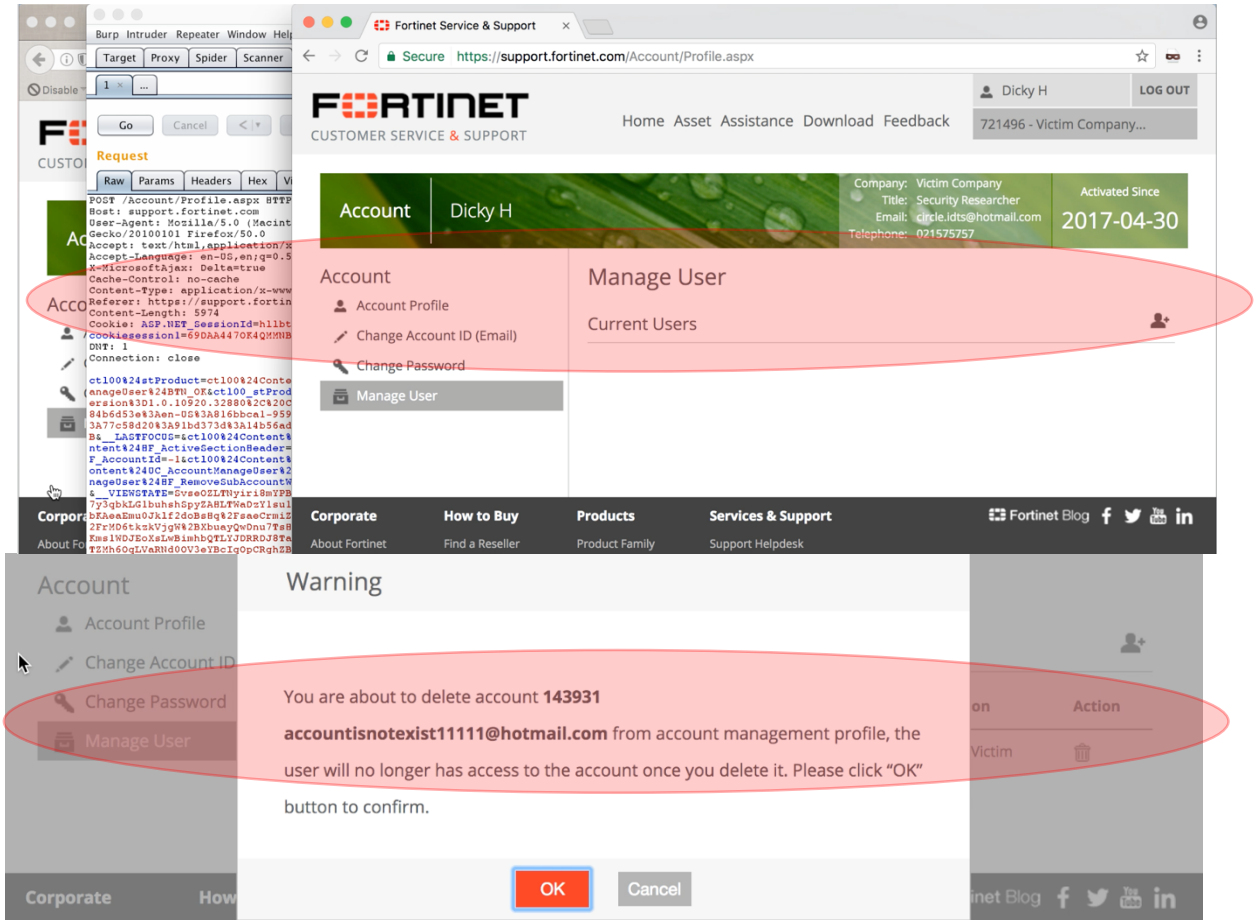
Unrestricted Deletion to All Other Sub Account via IDOR at FortiNet Support Portal



May 01st, 2017

@YoKoAcc (yk@firstsight.me)

[English Version]

Revision Detail

Version	Date	Detail
0.1	May 01st, 2017	-
0.2	May 04th, 2017	Added the timeline of reporting and fixed information

Table of Contents

Table of Figures

Table of Figures

I. ABSTRACT

As a part for completing the support to all the customer, FortiNet providing the support portal (located at: https://support.fortinet.com/Home.aspx) for their customer to communicate each other. One of the interesting feature that available at the Support Portal is "manage user" that could be used to connected with other account in one group (we will call it as sub-account creation).

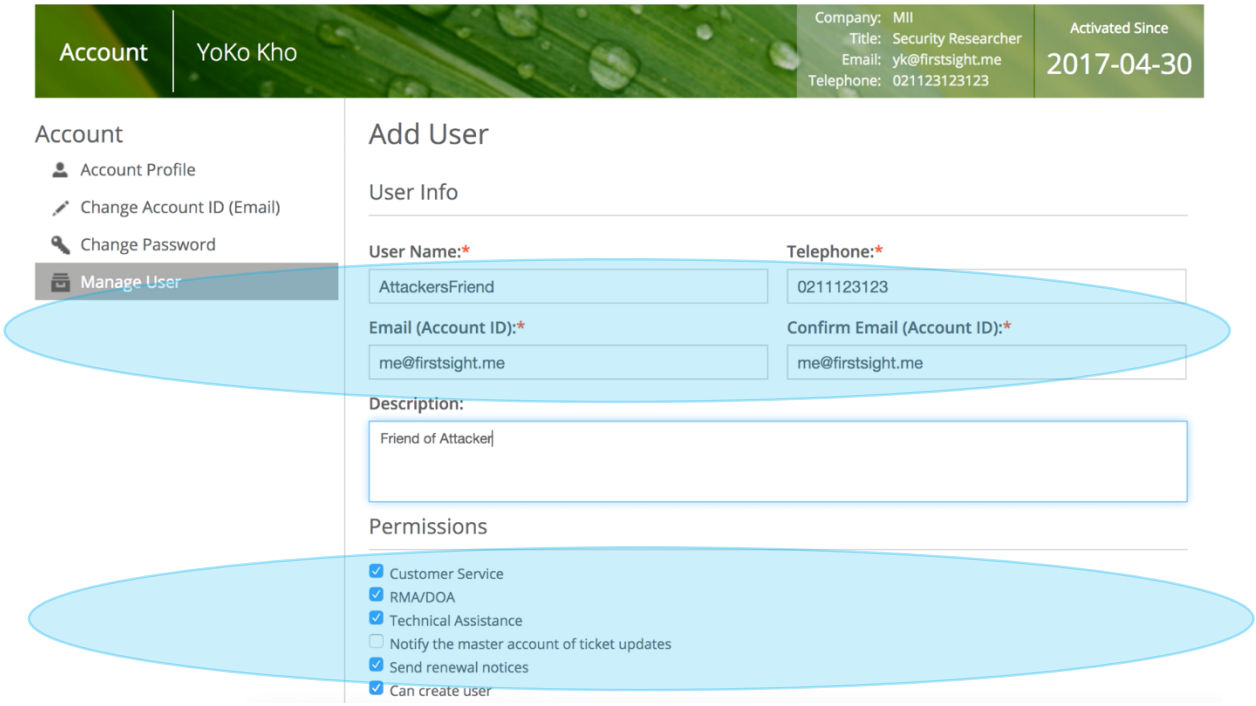


Figure 1 Manage User Feature at FortiNet's Support Portal

Once the sub-account is created, then the sub-account itself will automatically provide the sub-id number. Please kindly note that by default, this sub-id will appear in the front-end page when the administrator would like to delete / remove it from the group.

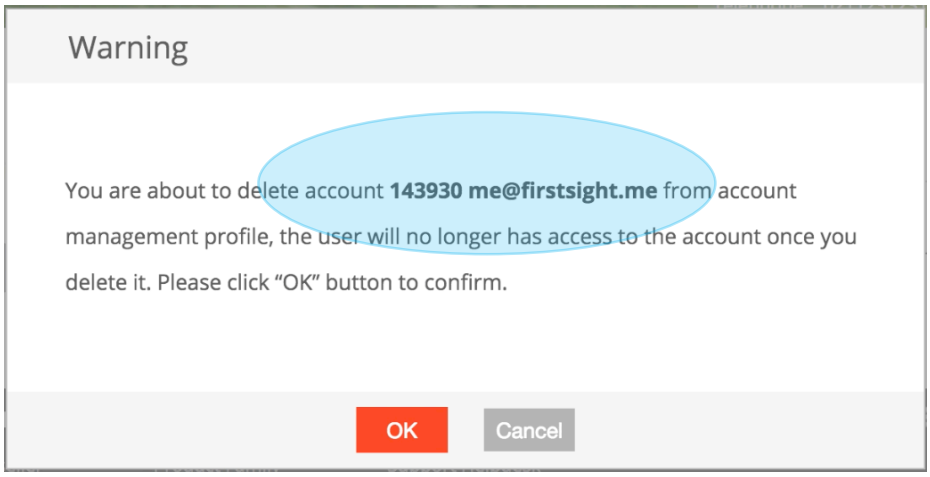


Figure 2 Sub-ID for the Sub-Account at the "Group"

As the previous picture shown, since the sub-account could be created at this portal by the "administrator" of the group, FortiNet also provides the feature to delete / remove the sub-account too. However, the problem occurs when FortiNet hasn't implemented the session limitation for customer to using the deletion / removal feature. In other words, the Attacker could delete any sub-account from other users (outside of the group) without the knowledge of the email ID and the password to login.

II. INTRODUCTION

2.1. **FortiNet's Support Portal**

As we could see from the portal directly, the FortiNet's Support Portal could be used by any registered user to create a ticket (for a comprehensive communication about the FortiNet's product) and to chat with the FortiNet's team for a general technical question.

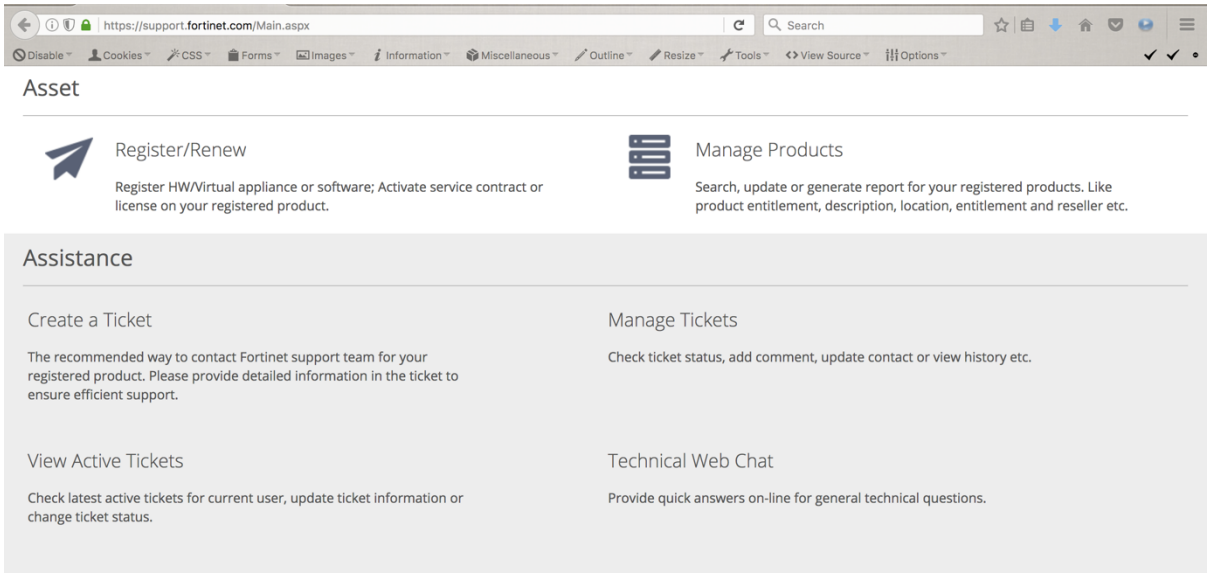


Figure 3 FortiNet's Support Portal Features

2.2. **Main Account and Sub Account**

As stated at the previous section, there are two difference account that could be created at the FortiNet's Support Portal. The first one could be used to act as an administrator of the group (which is the main account that provided with System ID). And the second one is the account that created by the Main Account, which is the Sub-Account that provided with the Sub-ID.

Since the picture of the Sub-ID has been provided at the previous section, then in this part, we will show only the System ID.

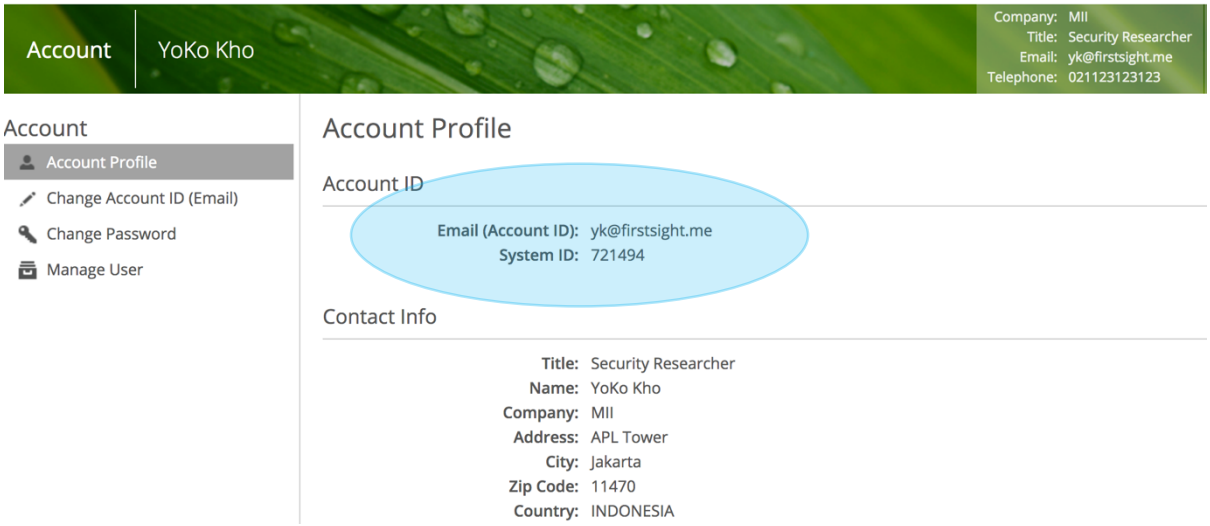


Figure 4 Sample of System ID (Main Account)

III. SUMMARY OF ISSUE

As it has been described, the security problem in this report is related to the vulnerability that "allows" an Attacker to be able to delete all sub-accounts that have been registered by the other main users in the FortiNet's Support Portal. It's important to be noted that the "benefit" in utilizing this vulnerability is the Attacker **doesn't need** any interactions from the user because they only need to change the **subid** parameter with their desired value.

IV. INFORMATION AND SITUATION OF THIS POC

To be able to understand the existed problem, this section will be re-explaining the problem specifically about some information which is related to the general running process or even the root of the existed problem. When a main user tries to delete their listed sub accounts, then the member is needed to confirm the deletion process. The sent request for confirming the deletion process is as follows:

```
POST /Account/Profile.aspx HTTP/1.1
Host: support.fortinet.com
User-Agent: User_Agent_here
```

```
Accept-Language: en-US,en;q=0.5

X-MicrosoftAjax: Delta=true

Cache-Control: no-cache

Content-Type: application/x-www-form-urlencoded; charset=utf-8

Referer: https://support.fortinet.com/Account/Profile.aspx

Content-Length: 5649

Cookie: cookies_over_here

DNT: 1

Connection: close


ctl00%24stProduct=value_here&ctl00_stProduct_HiddenField=value2_here&ctl00%24Content%24HF_ActiveSection=AccountManageUser&ctl00%24Content%24HF_ActiveSectionHeader=Account&ctl00%24Content%24UC_AccountSidebar%24HF_AccountId=-1&ctl00%24Content%24UC_AccountManageUser%24HF_Userid=-1&ctl00%24Content%24UC_AccountManageUser%24HF_Subid=143930&ctl00%24Content%24UC_AccountManageUser%24HF_RemoveSubAccountWarning_Control=&__EVENTTARGET=ctl00%24Content%24UC_AccountSidebar%24LinkButton1&__EVENTARGUMENT=&__VIEWSTATE=value3_here&__VIEWSTATEGENERATOR=value4_here&__EVENTVALIDATION=value5_here&__VIEWSTATEENCRYPTED=&__ASYNCPOST=true&
```

Table 1 Send a Request to Server when Confirming the Deletion

As can be seen from the table above, then we just need to change our "**Subid**" request to the Subid that we would like to change.

V. STEP TO REPRODUCE

Here is the simple scenario that made for providing the complete explanation:

5.1. Create two different main account. The 1st one will act as an Attacker (which is yk@firstsight.me) and the second one will act as a Victim (which is circle.idts@hotmail.com).

5.2. The next step is the Attacker create their sub-account (which is **me@firstsight.me**) and automatically got the Sub-ID from FortiNet: **143930**. And then, do the same thing with the Victim's Account. In this situation, the Victim's sub-account is **accountisnotexist111@hotmail.com** with the Sub-ID from FortiNet: **143931**.

5.3. The third step is, the Attacker tries to delete their sub-account with Sub-ID **143930** and intercept the request. When the application would like to send the deletion confirmation request (as could be seen at Table 1), then change the Sub-ID into the targeted ID, for example is **143931** (which is the sub-account from the Victim's account).

5.4. When the edited request has been send, then the deletion is completely successful.

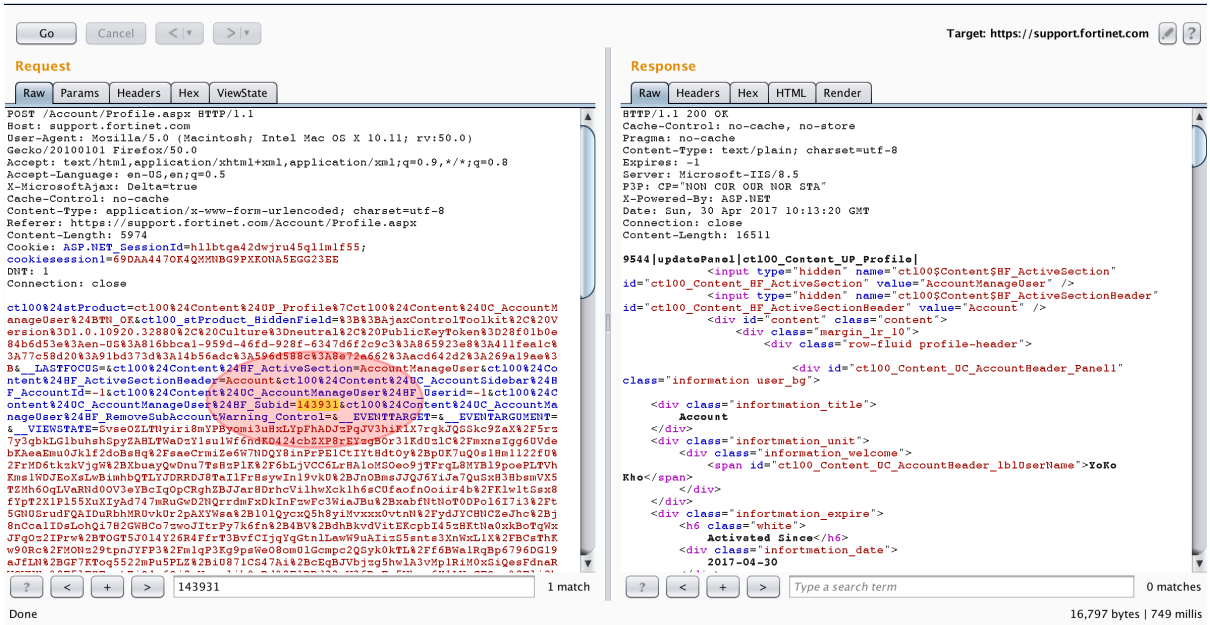


Figure 5 Intercept and Change the Sub-ID at Deletion Confirmation Request

5.5. Please kindly note, **the best part in this vulnerability is we can delete all the sub-account automatically in instant** with the intruder feature at Burpsuite. All we need just put the request from Sub-ID **#1** until Sub-ID **#143929**.

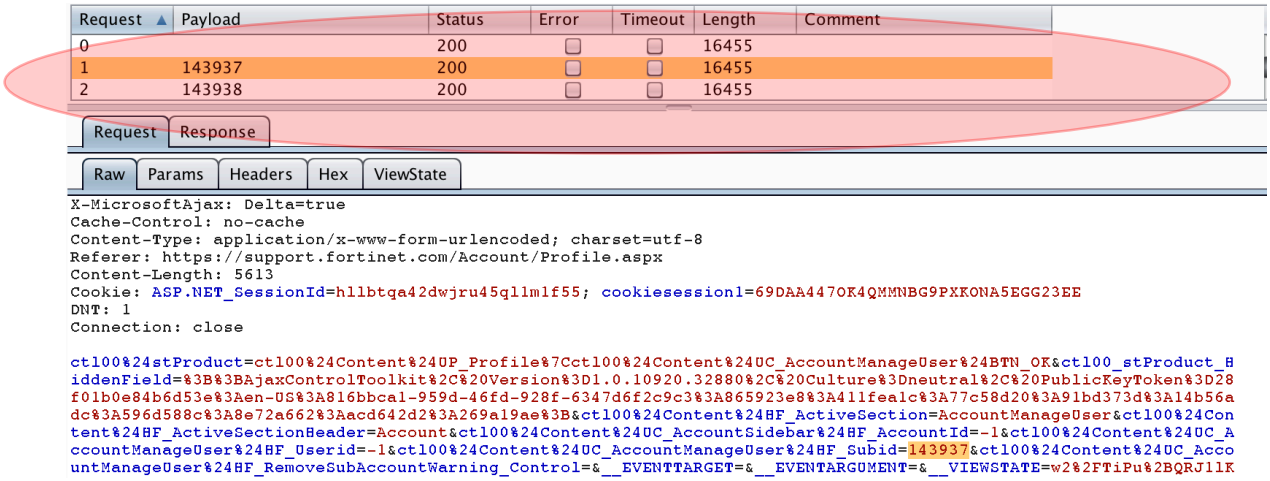


Figure 6 Example: The used of Intruder Feature

VI. RECOMMENDATION

In this situation, ensuring that every unique session / token is only functioning for its own account (couldn't be used by other users) would surely be a recommendation that can be implemented to cover the existed vulnerability.

VII. ADDITIONAL INFORMATION

For completing the explanation, here is the unlisted video that could be to explain the information related this vulnerability: https://www.youtube.com/watch?v=uMXhJhwwmz4

VIII. TIMELINE OF REPORTING

FortiNet has responded and deployed the fixed very fast. Only less than 24 hours after the report the first response from FortiNet's PSIRT team, the vulnerability successfully closed.

- May 01st, 2017 (09:06 AM, GMT+7) – Report v0.1 was sent via email;
- May 02nd, 2017 (05:22 AM, GMT+7) – First response from FortiNet and asked to resend the report;
- May 02nd, 2017 (05:56 AM, GMT+7) – Resend the report;
- May 02nd, 2017 (06:37 AM, GMT+7) – Confirming that PSIRT has received the report;
- May 03rd, 2017 (06:59 AM, GMT+7) – FortiNet said the vulnerability has been fixed and ask for the confirmation;
- May 03rd, 2017 (07:42 AM, GMT+7) – Confirming if the issue has been fixed and asking for public disclosure;
- May 04th, 2017 (04:26 AM, GMT+7) – FortiNet give the permission.

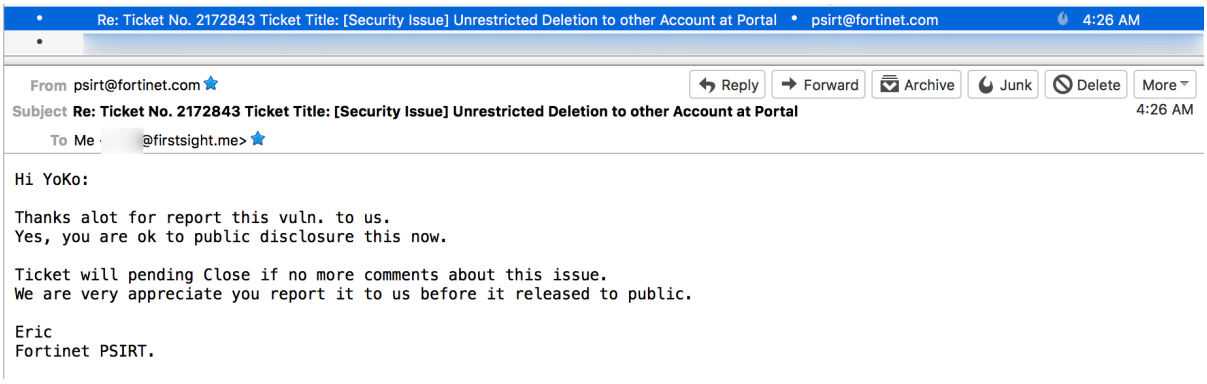


Figure 7 Permission to Publish the Article