Message

From: Schankweiler, Thomas W. (CMS/OIS) NotResp
NotResp
on behalf of Schankweiler, Thomas W. (CMS/OIS)
Sent: 12/9/2013 7:27:47 PM
To: Alexander, David (CMS/OIS NotResp
Subject: FW: HHS Request: IT Response Plans for 2 Tickets

David,

Here you go, do you need something further to complete the HHS form?

From: Schankweiler, Thomas W. (CMS/OIS)
Sent: Thursday, December 05, 2013 12:33 PM
To: Reinhold, Leslie A. (CMS/OEM); Fryer, Teresa M. (CMS/OIS)
Cc: Ambrosini, Ellen M. (CMS/OEM); Alexander, David (CMS/OIS); Wills, Theodora (CMS/OEM)
Subject: RE: HHS Request: IT Response Plans for 2 Tickets

All,

Here is the write up to close out 25244 in NotResp

Data.healthcare.gov
11/19 - Socrata investigated their platform for any signs of malicious activity. First, the activity referred to is the public user profile search API which doesn't reveal any private user information that could be exploited. Second, there is no connection or integration between Socrata platform user accounts and healthcare.gov user accounts. They are completely separate. Third, Socrate has been monitoring and there are no indications of any malicious activity targeting the Socrata platform or data.healthcare.gov.

Please close this as a False Positive -99

Thanks,

Tom

From: Schankweiler, Thomas W. (CMS/OIS)
Sent: Thursday, December 05, 2013 11:42 AM
To: Reinhold, Leslie A. (CMS/OEM); Fryer, Teresa M. (CMS/OIS)
Cc: Ambrosini, Ellen M. (CMS/OEM); Alexander, David (CMS/OIS); Wills, Theodora (CMS/OEM)
Subject: RE: HHS Request: IT Response Plans for 2 Tickets

The one for Balaji is no the 25244. If that the healthcare.data.gov then I has sent you the threads on that from OC and you were going to write it up.

From: Reinhold, Leslie A. (CMS/OEM)
Sent: Thursday, December 05, 2013 11:39 AM
To: Fryer, Teresa M. (CMS/OIS)
Cc: Ambrosini, Ellen M. (CMS/OEM); Alexander, David (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); Reinhold, Leslie A. (CMS/OEM); Wills, Theodora (CMS/OEM)
Subject: Re: HHS Request: IT Response Plans for 2 Tickets

Tom it's on that printout we looked at on Tuesday it's the last 2, NotResp that Balagi wrote up and data.gov. I know we discussed the data.gov one. Write up what the deal is with that if we are closing it let me know.

Thanks

On Dec 5, 2013, at 11:33 AM, "Fryer, Teresa M. (CMS/OIS)" <Teresa.Fryer@cms.hhs.gov> wrote:
Ellen,

What is #25244, Tom has indicated he does not know what this is and you have indicated that both tickets are for Marketplace.

Teresa

From: Ambrosini, Ellen M. (CMS/OEM)
Sent: Wednesday, December 04, 2013 6:58 PM
To: Fryer, Teresa M. (CMS/OIS); Alexander, David (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS)
Cc: Reinhold, Leslie A. (CMS/OEM); Wills, Theodora (CMS/OEM)
Subject: HHS Request: IT Response Plans for 2 Tickets
Importance: High

Good evening, Teresa-

We met with HHS today and they are requesting several HHS Response Plans on several tickets. Therefore, please complete a Response Plan (template attached) for the below two IT tickets from the Marketplace:

- NotResp # 24913, NotResp # INC000002589982 (see below for status)
- # 25244, N/A NotResp icket as this was entered by CMS IRT.

We will be preparing a Response Plan for several tickets covering an issue regarding potential PII violations and will ask you to review / input the IT section, as necessary.

All of these plans are due to the Department before COB on Friday, December 6th. We asked for an extension today and was told that the information is required on Friday.
Please let me know if you have any questions.

Thank you,

Ellen M. Ambrosini
Acting Director, Division of Privacy Policy

Privacy Policy Compliance Group, Office of E-Health Standards & Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244
410-786-6918

<image001.jpg>

INFORMATION NOT RELEASABLE TO THE PUBLIC UNLESS AUTHORIZED BY LAW: This information has not been publicly disclosed and may be privileged and confidential. It is for internal government use only and must not be disseminated, distributed, or copied to persons not authorized to receive the information. Unauthorized disclosure may result in prosecution to the full extent of the law.

From: Schankweiler, Thomas W. (CMS/OIS)
Sent: Tuesday, December 03, 2013 1:02 PM
To: Reinhold, Leslie A. (CMS/OEM)
Subject: Fw: INC000002589982

From: Ramamoorthy, Balaji Manikandan (CGI Federal) [mailto:balajimanikandan.ramamoorthy@cgifederal.com]
Sent: Tuesday, December 03, 2013 12:31 PM
To: Schankweiler, Thomas W. (CMS/OIS); Warren, Kevin (CMS/OIS); Lyles, Darrin V. (CMS/OIS); sbanks@foregroundsecurity.com <sbanks@foregroundsecurity.com>
Cc: FFM Security Defects <FFMSecurityDefects@cgifederal.com>; Martin, Rich (CGI Federal) <Rich.Martin@cgifederal.com>; Promisel, Andrew L (CGI Federal) <andy.promisel@cgifederal.com>; Alford, Justin (CGI Federal) <justin.alford@cgifederal.com>
Subject: INC000002589982

Hi Tom,

As discussed here is the write up for the incident # INC000002589982. Please forward it as necessary.

Issue:

An authenticated user can craft a NotResp the URL that provides the EligibilityNotice.pdf. If the NotResp on the system is not truly Unique, this could pose a risk of disclosure to users. Once logged into HealthCare.gov, a user could script a NotResp the system to retrieve any user's eligibility form.

Analysis:

A Proof of Concept was performed by the Marketplace Security Team where user A provided a URL to user B. User B was able to see the EligibilityNotice.pdf for User A.

Resolution:

FFM security team have put a code fix in place that will check the meta data of the notices stored in NotResp and make sure that it is associated with the user who is logged in before it could be downloaded by the user. The meta data for the notice includes the NotResp and the username. The fix accounts for different roles such as

1. Consumers
2. Agents/Brokers
3. CCR's
4. ESD workers.

The fix has been successfully tested in the lower environments for all these roles and the code has been promoted to the production. The enforcement has not been turned on in production due to the following reasons.

1. Currently the meta data is not populated for the notices stored in NotResp All the existing notices have to be updated for the meta data by the data cleanup team. This involves checking the NotResp for all notices, obtaining the NotResp and username and populating NotResp with proper meta data.
2. The development team has to update the code to make sure that any new notice generation is populating the proper meta data going forward.

Action Items

We don't have an ETA for these 2 tasks listed above and when the enforcement can be turned on. I have copied Justin Alford (who leads the data cleanup team) and Andy Promisel (who leads the development efforts) in the email as well.

Please let me know if you need more information.

Thanks
Balaji M. Ramamoorthy