Message

From: Schankweiler, Thomas W. (CMS/OIS) NotResp NotResp
on behalf of Schankweiler, Thomas W. (CMS/OIS)
Sent: 12/4/2013 7:48:12 PM
To: Fender, Rebecca (CMS/CCSQ) NotResp
Lyles, Darrin V. (CMS/OIS) NotResp NotResp Outerbridge, Monique (CMS/OIS) NotResp NotResp
CC: Grothe, Kirk A. (CMS/OIS) NotResp NotResp Outerbridge, Monique (CMS/OIS) NotResp NotResp Couts, Todd (CMS/OIS) NotResp NotResp
Michael Finkel [mfinkel@qssinc.com]
Subject: RE: Response Needed: Reactivation of Notice Link

Becca,

I cannot approve this at this time. ntil the NotResp fix is fully implemented and proven to be working. See the lingering issues that are listed below.

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 n 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

From: Fender, Rebecca (CMS/CCSQ)
Sent: Wednesday, December 04, 2013 2:45 PM
To: Lyles, Darrin V. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); Outerbridge, Monique (CMS/OIS)
Subject: FW: Response Needed: Reactivation of Notice Link
Importance: High

Tom/Darrin we need approval on this ASAP.

Becky Fender PMP®
CMS
Cell (b)(6)
Office 410-786-1006

From: Walker, Benjamin L. (CMS/CCIIO)
Sent: Wednesday, December 04, 2013 2:43 PM
To: Fender, Rebecca (CMS/CCSQ)
Subject: Fw: Response Needed: Reactivation of Notice Link
Importance: High

From: Mcveigh, Colin T. (CMS/CCIIO)
Sent: Tuesday, December 03, 2013 04:51 PM
To: Walker, Benjamin L. (CMS/CCIIO); Block, Lauren M. (CMS/CCIIO); Kane, Elizabeth M. (CMS/CCIIO); Camera, Ariella A. (CMS/CCIIO); Schankweiler, Thomas W. (CMS/OIS)
Subject: RE: Response Needed: Reactivation of Notice Link

Tom please see below. We need direction from security/privacy and are trying to move this as quickly as possible.

Thanks!

Colin McVeigh
Center for Consumer Information and Insurance Oversight
301.492.4263

From: Mcveigh, Colin T. (CMS/CCIIO)
Sent: Tuesday, December 03, 2013 11:26 AM
To: Walker, Benjamin L. (CMS/CCIIO); Block, Lauren M. (CMS/CCIIO); Kane, Elizabeth M. (CMS/CCIIO); Camera, Ariella A. (CMS/CCIIO); Schankweiler, Thomas W. (CMS/OIS)
Subject: RE: Response Needed: Reactivation of Notice Link

Hi Tom,

There is a privacy/security issue detailed below which we'd like you to weigh in on. At this point, we think the best course of action is to reactive the notice link.

Thanks!

Colin McVeigh
Center for Consumer Information and Insurance Oversight
301.492.4263

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: Walker, Benjamin L. (CMS/CCIIO)
Sent: Tuesday, December 03, 2013 10:29 AM
To: Mcveigh, Colin T. (CMS/CCIIO); Block, Lauren M. (CMS/CCIIO); Kane, Elizabeth M. (CMS/CCIIO); Camera, Ariella A. (CMS/CCIIO)
Subject: Re: Response Needed: Reactivation of Notice Link

I support re-activating it. I think Tom Schankweiler needs to weigh in.

From: Mcveigh, Colin T. (CMS/CCIIO)
Sent: Tuesday, December 03, 2013 10:17 AM
To: Block, Lauren M. (CMS/CCIIO); Walker, Benjamin L. (CMS/CCIIO); Kane, Elizabeth M. (CMS/CCIIO); Camera, Ariella A. (CMS/CCIIO)
Subject: Response Needed: Reactivation of Notice Link

Hi all,

More than a month ago we received reports that consumers were seeing other consumer's notices through a link on the application that should have taken them to their own determination notice. After receiving those reports, CGI decided to deactivate the problematic link.

Since then, a number of related fixes have been made although none directly addressing this particular notice issue. Additionally, CGI has never been able to recreate this issue in lower environments because of the way those environments are configured and how they are accessed internally. Our CGI development lead (Stephen Wass) believes that this issue is likely fixed at this point. However, since it was not something that could be reproduced here we cannot be sure. At this point, CGI needs CMS guidance regarding whether or not to reactivate the link.

Lauren, I'm not sure who has the authority to make this call but I was hoping you might be able to push it in the right direction. I've laid out some pros and cons regarding reactivating the link or keeping it inactive below.

Activating the Link

- Consumers can receive the link and their notice as designed.
- Developers believe it is likely resolved.
- Because we have not been able to reproduce the issue in lower environments, activating the link and then listening for 'noise' on this issue may be the most effective way to determine whether it is fixed or not.
- The issue may not be fixed and privacy risks may surface.

Keeping Link Inactive

- This would negate privacy risks above.
- Consumers would lose one avenue through which they can learn about their determination.
- Since this defect has not been reproducible on our end, it will be difficult to confirm whether or not the defect is actually fixed without actually activating the link in production.

If anyone else has any other information to add to this issue please feel free.

Thanks!

Colin McVeigh
Center for Consumer Information and Insurance Oversight
301.492.4263