Message

From: Schankweiler, Thomas W. (CMS/OIS NotResp
NotResp
on behalf of Schankweiler, Thomas W. (CMS/OIS)
Sent: 12/4/2013 2:59:41 AM
To: Peterson, Jason R. (CMS/CTR) NotResp
NotResp
Subject: FW: Security Items that Need Attention
Attachments: NotResp Ticket Status Update Requested by CMS 120313.docx

FYI

From: Goodrich, Lynn F (CGI Federal) [mailto:lynn.goodrich@cgifederal.com]
Sent: Tuesday, December 03, 2013 9:21 PM
To: Outerbridge, Monique (CMS/OIS); Kane, David (CMS/OIS); Couts, Todd (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); mfinkel@qssinc.com; sbanks@foregroundsecurity.com; Warren, Kevin (CMS/OIS); Fletcher, John A. (CMS/OIS); Van, Hung B. (CMS/OIS); Grothe, Kirk A. (CMS/OIS); Lyles, Darrin V. (CMS/OIS); vnatarajan@qssinc.com; Kirk, Thomas (GSS-CGI); Martin, Rich (CGI Federal)
Cc: FFM Security Defects
Subject: RE: Security Items that Need Attention

Please find attached a detailed update of the NotResp tickets referenced in #2 below as well as some additional ones opened that day missing from the list.

Please let me know if you have any questions.

Thanks.

Lynn Goodrich
IT Security Manager | **CGI Federal** Health & Compliance Security Practice (HCSP) | Cell: (b)(6) Office: 703-227-5568 | Lynn.Goodrich@cgifederal.com

From: Martin, Rich (CGI Federal)
Sent: Tuesday, December 03, 2013 9:17 AM
To: Krishnan, Venkatesh (CGI Federal); Goodrich, Lynn F (CGI Federal)
Cc: Ramamoorthy, Balaji Manikandan (CGI Federal)
Subject: FW: Security Items that Need Attention

Hi folks – please see below email trail. There are a number of security incidents/defects various people at CMS are seeking updates for? Can you please verify those NotResp umbers and determine which are defects assigned to us and which are POAMs. Also, we can use this as the basis for or status report internally and ultimately to CMS – all will want a dashboard backed up by detail list. Please let me know ASAP. Thank you.

From: Kirk, Thomas (GSS-CGI)
Sent: Tuesday, December 03, 2013 8:09 AM
To: Martin, Rich (CGI Federal)
Subject: FW: Security Items that Need Attention

Tom Kirk | Government Secure Solutions CGI Inc. (b)(6) cell | tom.kirk@cgifederal.com

From: Outerbridge, Monique (CMS/OIS) [mailto:monique.outerbridge@cms.hhs.gov]
Sent: Tuesday, December 03, 2013 8:07 AM
To: Ramamoorthy, Balaji Manikandan (CGI Federal); Kane, David (CMS/OIS); Couts, Todd (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); Michael Finkel; sbanks@foregroundsecurity.com
Cc: Warren, Kevin (CMS/OIS); Fletcher, John A. (CMS/OIS); Van, Hung B. (CMS/OIS); Grothe, Kirk A. (CMS/OIS); Lyles, Darrin V. (CMS/OIS); 'Venky Natarajan' (vnatarajan@qssinc.com) (vnatarajan@qssinc.com); Goodrich, Lynn F (CGI Federal); Kirk, Thomas (GSS-CGI)
Subject: RE: Security Items that Need Attention

Hey guys. Has this security issue been resolved yet? This is very important and needs to happen asap.

From: Ramamoorthy, Balaji Manikandan (CGI Federal) [balajimanikandan.ramamoorthy@cgifederal.com]
Sent: Wednesday, November 27, 2013 2:48 PM
To: Kane, David (CMS/OIS); Couts, Todd (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); Michael Finkel; sbanks@foregroundsecurity.com
Cc: Warren, Kevin (CMS/OIS); Fletcher, John A. (CMS/OIS); Van, Hung B. (CMS/OIS); Grothe, Kirk A. (CMS/OIS); Lyles, Darrin V. (CMS/OIS); 'Venky Natarajan' (vnatarajan@qssinc.com) (vnatarajan@qssinc.com); Goodrich, Lynn F (CGI Federal); Kirk, Thomas (GSS-CGI); Outerbridge, Monique (CMS/OIS)
Subject: RE: Security Items that Need Attention
Including Stacy Banks.

Thanks
Balaji M. Ramamoorthy

From: Kane, David (CMS/OIS) [mailto:David.Kane@cms.hhs.gov]
Sent: Wednesday, November 27, 2013 2:35 PM
To: Todd.Couts1; Schankweiler, Thomas W. (CMS/OIS); Michael Finkel
Cc: Warren, Kevin (CMS/OIS); Fletcher, John A. (CMS/OIS); Van, Hung B. (CMS/OIS); kirk.grothe; Lyles, Darrin V. (CMS/OIS); 'Venky Natarajan' (vnatarajan@qssinc.com) (vnatarajan@qssinc.com); Goodrich, Lynn F (CGI Federal); Kirk, Thomas (GSS-CGI); Ramamoorthy, Balaji Manikandan (CGI Federal); monique.outerbridge
Subject: RE: Security Items that Need Attention

Todd,

Did we receive a response indicating the status of each? Please advise.

Respectfully,

DAVID KANE
Office: 410-786-1193

BB: (b)(6)
David.Kane@cms.hhs.gov

From: Couts, Todd (CMS/OIS)
Sent: Tuesday, November 26, 2013 3:48 PM
To: Schankweiler, Thomas W. (CMS/OIS); Kane, David (CMS/OIS); Michael Finkel
Cc: Warren, Kevin (CMS/OIS); Fletcher, John A. (CMS/OIS); Van, Hung B. (CMS/OIS); Grothe, Kirk A. (CMS/OIS); Lyles, Darrin V. (CMS/OIS); 'Venky Natarajan' (vnatarajan@qssinc.com) (vnatarajan@qssinc.com); lynn.goodrich@cgifederal.com; Thomas.Kirk@gss-cgi.com; 'Ramamoorthy, Balaji Manikandan (CGI Federal)' (balajimanikandan.ramamoorthy@cgifederal.com); Outerbridge, Monique (CMS/OIS)
Subject: Security Items that Need Attention

QSSI and CGI,

I am writing to highlight several security incidents that need your attention. As they are security issues, please consider the NotResp ticket your authorization to act. I am only sending the Remedy numbers to avoid transmitting too much detail. By tomorrow, please communicate back to use their status (closed, in process, etc) and at least a tentative date for resolution.

1. These are the two that Tom Schankweiler raised today.
   - INC000002589982
   - artf161265 INC2598675

2. Additionally, we identified several open tickets in NotResp
   - 2614246
   - 2614253
   - 2614255
   - 2614297
   - 2614299
   - 2614303
   - 2614304
   - 2614305
   - 2614307
   - 2614309
   - 2614310
   - 2614311
   - 2614313
   - 2614316
   - 2614317
   - 2614318
   - 2614319
   - 2614320
   - 2614321
   - 2614322
   - 2614323
   - 2614324
   - 2614325
   - 2614326
   - 2614328
   - 2614329
   - 2614330
   - 2614331
   - 2614332
   - 2614327
   - 2614333

- 2614334
- 2614335
- 2614336
- 2614337
- 2614338
- 2614339
- 2614340
- 2614341

Todd Couts
Centers for Medicare & Medicaid Services
Office of Information Services
301-492-5139 (office) | (b)(6) (mobile) | todd.couts1@cms.hhs.gov
7700 Wisconsin Ave Bethesda MD 20814 | Location: 9308

From: Schankweiler, Thomas W. (CMS/OIS)
Sent: Tuesday, November 26, 2013 12:41 PM
To: Couts, Todd (CMS/OIS); Kane, David (CMS/OIS); Michael Finkel
Cc: Warren, Kevin (CMS/OIS); Fletcher, John A. (CMS/OIS); Van, Hung B. (CMS/OIS); Grothe, Kirk A. (CMS/OIS); Lyles, Darrin V. (CMS/OIS)
Subject: INC000002589982 Need details regarding DocumentFromECM?fileIdentifier=

Todd,

I would like to escalate this ticket NC000002589982 as being high risk on the defect list. I know that a bunch of security risk have recently appeared on the list but I wanted to let you know this one is considered high priority. In total we now have two tickets that are considered high priority. Contact me if you have any questions.

Thanks,

Tom

From: Ramamoorthy, Balaji Manikandan (CGI Federal) [mailto:balajimanikandan.ramamoorthy@cgifederal.com]
Sent: Tuesday, November 26, 2013 10:52 AM
To: Schankweiler, Thomas W. (CMS/OIS); Willard, Adam (CMS/CTR)
Cc: Warren, Kevin (CMS/OIS); Quaintance, Eric (CGI Federal); Dhas, Navin (CGI Federal); Alford, Justin (CGI Federal); Martin, Rich (CGI Federal)
Subject: RE: artf160711 / INC000002589982 Need details regarding DocumentFromECM?fileIdentifier=

Hi Tom,
We promoted the code fix into production. Apparently the security enforcement is turned off.

The NotResp documents (notices) that are saved are not having the proper meta data populated to turn on the enforcements. So in addition to the fix that has been rolled in the following actions needs to occur.

1. Do a manual batch job to update the meta data for all the existing notices.
2. Have the developers fix the code so that any new notices that are saved has the proper metadata for enforcement.

These 2 action items are being coordinated internally right now. We don't have an ETA yet.

Thanks
Balaji M. Ramamoorthy

From: Schankweiler, Thomas W. (CMS/OIS) [mailto:thomas.schankweiler@cms.hhs.gov]
Sent: Tuesday, November 26, 2013 10:42 AM
To: Ramamoorthy, Balaji Manikandan (CGI Federal); Willard, Adam (CMS/CTR)
Cc: Warren, Kevin (CMS/OIS); Quaintance, Eric (CGI Federal); Dhas, Navin (CGI Federal)
Subject: artf160711 / INC000002589982 Need details regarding DocumentFromECM?fileIdentifier=

Balaji, Adam, and Kevin

I am looking for an update on this ticket. Can someone provide be a status of where we are with this item? Has it been corrected? Is the situation still occurring?

Thanks,

Tom

From: Ramamoorthy, Balaji Manikandan (CGI Federal) [mailto:balajimanikandan.ramamoorthy@cgifederal.com]
Sent: Wednesday, November 06, 2013 12:39 PM
To: Willard, Adam (CMS/CTR)
Cc: Warren, Kevin (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); Quaintance, Eric (CGI Federal); Dhas, Navin (CGI Federal)
Subject: RE: Need details regarding DocumentFromECM?fileIdentifier=

Hi Adam,
There are multiple instances of NotResp We expect NotResp guarantees for the uniqueness across JVM's. We did go this route to see if there were duplicates.

So far the root cause has not been determined for the notices. In this particular instance we did see that the username were closely identical between the user1 and user2. There was a special character "-" at the end (and that was the only difference). We are also looking into the NotResp to see how it behaves and whether it has to be tweaked.

Thanks
Balaji M. Ramamoorthy

From: Willard, Adam (CMS/CTR) [mailto:Adam.Willard@cms.hhs.gov]
Sent: Wednesday, November 06, 2013 12:05 PM
To: Ramamoorthy, Balaji Manikandan (CGI Federal)
Cc: Warren, Kevin (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); Quaintance, Eric (CGI Federal); Dhas, Navin (CGI Federal)
Subject: RE: Need details regarding DocumentFromECM?fileIdentifier=

Is NotResp just 1 instance or are there several instances in production? If there are multiple systems generating a GUID there could be collisions.

What was the analysis from the Users who said they saw someone's Notice instead of theirs. Was there any check to see if the GUID for that user and the other user was the same?

Adam Willard (Contractor)
703-354-2229 x513 (Direct)
(b)(6) (Mobile)
Adam.Willard@cms.hhs.gov

CMS XOC Security Team
Consumer Information & Insurance Systems Group (CIISG)
Centers for Medicare & Medicaid Services (CMS)
703-594-4961/703-910-3993
ciisg-soc@cms.hhs.gov

From: Ramamoorthy, Balaji Manikandan (CGI Federal) [balajimanikandan.ramamoorthy@cgifederal.com]
Sent: Wednesday, November 06, 2013 11:47 AM
To: Willard, Adam (CMS/CTR)
Cc: Warren, Kevin (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); Quaintance, Eric (CGI Federal); Dhas, Navin (CGI Federal)
Subject: RE: Need details regarding DocumentFromECM?fileIdentifier=

Hi Adam,

The eligibility notices are stored in NotResp and the URI's for the notices are stored against the user record in NotResp

The GUID for the PDF document itself is generated by NotResp and it is sufficiently random.

We did identify this issue internally and it is in the list of high priority items to be fixed. I will track down on the ETA for the fix and let you know.

I agree that in the meantime to see if the rate control can be applied to this specific URL.

Thanks
Balaji M. Ramamoorthy

From: Willard, Adam (CMS/CTR) [mailto:Adam.Willard@cms.hhs.gov]
Sent: Wednesday, November 06, 2013 9:37 AM
To: Ramamoorthy, Balaji Manikandan (CGI Federal)
Cc: Warren, Kevin (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); Quaintance, Eric (CGI Federal)
Subject: Need details regarding DocumentFromECM?fileIdentifier=
Importance: High

Balaji,

I noticed this morning that it is possible for anyone to run a brute force against healthcare.gov to obtain the results of their eligibility.

I need to know where you are grabbing the file from (NotResp or something else). Is that system publicly accessible?

We need to know if there is anyway to put in permission checking of the workspace url GUID against the list of possible GUIDs for a user.

I sent Shima (an XOC Security Analyst) my eligibility URL and she was able to see my results in PDF format.

We are looking into a Rate Control for the NotResp to block or limit access to this screen if several attempts are made over X period of time.

Adam Willard (Contractor)
703-354-2229 x513 (Direct)
(b)(6) (Mobile)
Adam.Willard@cms.hhs.gov

CMS XOC Security Team
Consumer Information & Insurance Systems Group (CIISG)
Centers for Medicare & Medicaid Services (CMS)
703-594-4961/703-910-3993
ciisg-soc@cms.hhs.gov