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.