Message

From: Linares, George E. (CMS/OIS) NotResp NotResp
Sent: 12/17/2013 4:37:57 PM
To: Steiner, Chip [frank.steiner@noblis.org]; Schankweiler, Thomas W. (CMS/OIS) NotResp NotResp chatoff, Jack H. (CMS/OIS) NotResp NotResp ; Feuerberg, Lisa A.(CMS/OIS) NotResp NotResp Warren, Kevin (CMS/OIS) NotResp NotResp
CC: Cappelletti, John Danilo [john.cappelletti@noblis.org]
Subject: RE: ACA testing report

All,
Even if the report is to be completed on a bi-weekly basis, the actual monitoring and pen testing needs to occur on a weekly basis as per the Decision Memo. I don't think we have any flexibility on that regard. So let's make sure that it happens weekly.

Thanks

George Linares
Acting Chief Technology Officer
Centers for Medicare & Medicaid Services (CMS)
410.786.2866 george.linares@cms.hhs.gov
7500 Security Blvd., N3-15-25
Baltimore, MD 21244-1850

Need more information? Visit the OIS website.

From: Steiner, Chip [mailto:frank.steiner@noblis.org]
Sent: Tuesday, December 17, 2013 9:41 AM
To: Schankweiler, Thomas W. (CMS/OIS); Schatoff, Jack H. (CMS/OIS); Feuerberg, Lisa A.(CMS/OIS); Warren, Kevin (CMS/OIS)
Cc: Linares, George E. (CMS/OIS); Cappelletti, John Danilo
Subject: RE: ACA testing report

George,

The Security Decision Memo that we are addressing states:

- *Monitor and perform the weekly testing of all border devices, including internet facing web servers;*

The HROB weekly status report states:
Penetration testing is conducted weekly from an external Internet Protocol (IP) address not associated with CMS or any .gov entity. The Internet-facing Web servers that comprise the FFM environment and are penetration tested are located at the following application Uniform Resource Locators (URLs):

- *www.healthcare.gov/marketplace*
- *https://www.cuidadodesalud.gov/es/*

I believe that we've stated in the past that testing would alternate weekly between the english and spanish sites. In addition, we still have the statement in the HROB weekly status report that testing of the firewalls that has been included since the original HROB report:

Penetration testing of network infrastructure devices (specifically, two redundant firewalls) will be underway shortly, pending coordination with the Terremark datacenter.

C.

From: Schankweiler, Thomas W. (CMS/OIS) [thomas.schankweiler@cms.hhs.gov]
Sent: Tuesday, December 17, 2013 9:19 AM
To: Schatoff, Jack H. (CMS/OIS); Feuerberg, Lisa A.(CMS/OIS); Warren, Kevin (CMS/OIS)
Cc: Linares, George E. (CMS/OIS); Cappelletti, John Danilo; Steiner, Chip
Subject: RE: ACA testing report

Jack,

Please let Kevin know which systems you need credentials for, and he can work on the coordination to get this for you.

George, I think if you end up making the HRoB report an bi-weekly delivery that the scan schedule for HC.gov will fit nicely.

Tom

From: Schatoff, Jack H. (CMS/OIS)
Sent: Tuesday, December 17, 2013 9:14 AM
To: Schankweiler, Thomas W. (CMS/OIS); Feuerberg, Lisa A.(CMS/OIS)
Cc: Linares, George E. (CMS/OIS); Cappelletti, John Danilo; Steiner, Chip
Subject: RE: ACA testing report

Tom,

Due to the large number of ACA sites, including satellite sites, my one tester can only thoroughly test a certain number of web sites each week. With that said, we hit the healthcare.gov site once every two weeks. We can hit it every week, but that will cause other ACA sites to be tested less frequently.

EISG could perform better testing if we had user credentials on all of the ACA systems.

Please advise.

Thanks,

Jack

From: Schankweiler, Thomas W. (CMS/OIS)
Sent: Monday, December 16, 2013 2:21 PM
To: Feuerberg, Lisa A.(CMS/OIS)
Cc: Linares, George E. (CMS/OIS); Schatoff, Jack H. (CMS/OIS); Cappelletti, John Danilo; Steiner, Chip
Subject: RE: ACA testing report

Jack,

I'll leave this one to you…

Tom

From: Feuerberg, Lisa A.(CMS/OIS)
Sent: Monday, December 16, 2013 2:15 PM
To: Schankweiler, Thomas W. (CMS/OIS)
Cc: Linares, George E. (CMS/OIS); Schatoff, Jack H. (CMS/OIS); Cappelletti, John Danilo; Steiner, Chip
Subject: RE: ACA testing report

Hi Tom:

Can you let us know why the scans didn't target healthcare.cov? We're anticipating that question from the recipients of the HROB which includes the administrator and OIG.

Lisa Feuerberg
Centers for Medicare & Medicaid Services (CMS)
Office of Information Services (OIS)
Information Services Design & Development Group (IHDSG)
☎ 410.786.6840 (O (b)(6)
✉ lisa.feuerberg@cms.hhs.gov
7500 Security Blvd., N3-17-26
Baltimore, MD 21244-1850

Need more information? Please visit the OIS website.

From: Schankweiler, Thomas W. (CMS/OIS)
Sent: Friday, December 13, 2013 3:15 PM
To: Steiner, Chip
Cc: Linares, George E. (CMS/OIS); Schatoff, Jack H. (CMS/OIS); Feuerberg, Lisa A.(CMS/OIS); Cappelletti, John Danilo
Subject: RE: ACA testing report

Chip,

The scans from this week did not target healthcare.gov

The finder page shares the same namespace, but is actually tied to the HIOS application.

There would be no new findings for the HRob report for this week.

Tom

From: Steiner, Chip [mailto:frank.steiner@noblis.org]
Sent: Friday, December 13, 2013 11:24 AM
To: Schankweiler, Thomas W. (CMS/OIS)
Cc: Linares, George E. (CMS/OIS); Schatoff, Jack H. (CMS/OIS); Feuerberg, Lisa A.(CMS/OIS); Cappelletti, John Danilo
Subject: [WARNING : MESSAGE ENCRYPTED] FW: ACA testing report

Tom,

I didn't get this report until after the meeting started this morning so I couldn't ask about the details, but it appears that we did not test the specific urls that we list in the status report [Jack - please correct me if this is not the case]. However, the associated url was tested:

https: NotResp

How should the following paragraphs be updated in the weekly status report to reflect this change?

Procedure

The dedicated security team conducts ongoing vulnerability assessments of the FFM network infrastructure and Internet-facing Web servers through penetration testing and monitoring. The purpose of this ongoing testing is to identify exploitable vulnerabilities present within devices that are used to support the Affordable Care Act. Identified vulnerabilities are managed, tracked, and resolved using the established CMS vulnerability management processes, details of which are provided below.

Penetration testing is conducted weekly from an external Internet Protocol (IP) address not associated with CMS or any .gov entity. The Internet-facing Web servers that comprise the FFM environment and are penetration tested are located at the following application Uniform Resource Locators (URLs):

- www.healthcare.gov/marketplace
- https://www.cuidadodesalud.gov/es/

Results

During this reporting period, penetration testing of Internet-facing Web servers identified no high or moderate vulnerabilities within FFM. Vulnerabilities identified in prior reports that have not been closed continue to be worked per the processes described above.

We also need an update of the following paragraph:

Penetration testing of network infrastructure devices (specifically, two redundant firewalls) will be underway shortly, pending coordination with the Terremark datacenter. The firewall devices are not publically accessible and require coordination with datacenter contractors to create the internal tunnels necessary to support this scanning activity.

I appreciate your help in completing this update.

C.

Chip Steiner | Senior Principal
Noblis | 3150 Fairview Park Drive South | Falls Church, Virginia | 22042-4519
o: 703.610.1574 | f: 703.610.1702 | chip.steiner@noblis.org

From: Kellison, Daryl L. (CMS/CTR) [Daryl.Kellison@cms.hhs.gov]
Sent: Friday, December 13, 2013 10:31 AM
To: Steiner, Chip
Subject: FW: ACA testing report

From: Kellison, Daryl L. (CMS/CTR)
Sent: Thursday, December 12, 2013 10:52 AM
To: Fryer, Teresa M. (CMS/OIS); Marantan, James (CMS/OIS); Elky, Mark (CMS/OIS); john.cappalletti@noblis.org; Schankweiler, Thomas W. (CMS/OIS); Lyles, Darrin V. (CMS/OIS); Feuerberg, Lisa A.(CMS/OIS); Linares, George E. (CMS/OIS)
Cc: Schatoff, Jack H. (CMS/OIS); Kreider, Brett (CMS/CTR); Conte, Michael B. (CMS/CTR); bryce.kunz@defpoint.com
Subject: ACA testing report
All

Attached is the report and CFACTS input for all applications supporting the ACA which were tested this week. The password to open the files will follow.

Thanks

Dary