



Catherine Judith Perez Coronado <cjperezc@colpensiones.gov.co>

Fwd: Servicio Web expuesto en internet Sobre HTTPS - Asalud

1 message

Arley Fabian Pinzon Vera <afpinzonv@colpensiones.gov.co>
To: Catherine Judith Perez Coronado <cjperezc@colpensiones.gov.co>

Fri, Jan 26, 2024 at 7:42 AM

pruebas Asalud

----- Forwarded message -----

De: **Diana Carolina Cardenas Leon** <dccardenasl@colpensiones.gov.co>
Date: vie, 26 ene 2024 a las 7:05
Subject: Fwd: Servicio Web expuesto en internet Sobre HTTPS - Asalud
To: Arley Fabian Pinzon Vera <afpinzonv@colpensiones.gov.co>

----- Forwarded message -----

De: **Arley Fabian Pinzon Vera** <afpinzonv@colpensiones.gov.co>
Date: mié, 14 dic 2016 a las 18:12
Subject: Re: Servicio Web expuesto en internet Sobre HTTPS - Asalud
To: Ing. Johana Pedraza <sistemas@asaludltda.com>, Adriana Sarmiento Nicholls <asarmienton@colpensiones.gov.co>, Diana Carolina Cardenas Leon <dccardenasl@colpensiones.gov.co>, Dr. Gabriel Vivas <gerenciaoperativa@asaludltda.com>
Cc: Nelsy Angarita <nangarita@colpensiones.gov.co>, John Alexander Fajardo Rincon <jafajardor@colpensiones.gov.co>, Luis Fernando Ucros Velasquez <lfucrosv@colpensiones.gov.co>, Ingrid Carolina Ariza Cristancho <icarizac@colpensiones.gov.co>, Alexander Estacio Moreno <aestaciom@colpensiones.gov.co>, Felipe Eduardo Gallon Medina <fegallonm@colpensiones.gov.co>, Paula Marcela Cardona Ruiz <pmcardonar@colpensiones.gov.co>, Angela Cristina Tobar Gonzalez <atobar@colpensiones.gov.co>, Alberto Barajas Ramon <abarajasr@colpensiones.gov.co>

Buenas tardes,

En relación al correo que antecede, seguridad informática informa que es viable la comunicación a través del Web Service y ya se pueden movilizar los casos.

Agradecemos su colaboración.

Gracias.

El 14 de diciembre de 2016, 18:05, Alberto Barajas Ramon <abarajasr@colpensiones.gov.co> escribió:

Buen dia,

Se adjuntan las evidencias de las pruebas realizadas:

URL: <https://wscolpproduccion.aplicativoasalud.com/INTEGRACIONService/IntegracionService.svc>URL: <https://wscolpproduccion.aplicativoasalud.com/INTEGRACIONService/IntegracionService.svc?wsdl>Servidor: wscolpproduccion.aplicativoasalud.com (64.37.63.202)

Se puede evidenciar en los reportes adjuntos, sobre la mejora sustancial en los servicios y vulnerabilidades hallados con anterioridad, se considera que ya es viable hacer uso de los servicios tipo WebService entre ASalud y Colpensiones, colpensiones en sus procesos de aseguramiento puede realizar estas pruebas más adelante como medida de control, cualquier duda con gusto sera resuelta, gracias.

Saludos cordiales,



Alberto Barajas Ramón

Asesor de Vicepresidencia

Vicepresidencia de Operaciones y Tecnología

Carrera 10 N° 72 – 33 Torre B Piso 7º

Teléfono: (57+1) 2170100 Ext. 1516

E-mail: abarajasr@colpensiones.gov.co

<https://www.colpensiones.gov.co>

Bogotá D.C. – Colombia

El 14 de diciembre de 2016, 16:08, Nelsy Angarita <nangarita@colpensiones.gov.co> escribió:

Buenas tardes

En este momento el grupo de seguridad de la VOT inicia la ejecución de pruebas de vulnerabilidad y sobre las 5pm tendremos el informe y concepto sobre las mismas.

Quedamos atentos

El 14 de diciembre de 2016, 15:55, Arley Fabian Pinzon Vera <afpinzonv@colpensiones.gov.co> escribió:

Buenas tardes,

Asalud realiza la corrección a los incidentes de vulnerabilidad con el fin de que la VOT, grupo de seguridad informática realice la prueba.

Solicitamos la misma se aplique cuanto antes con el fin de validar y abrir los puertos para la comunicación.

Gracias.

----- Mensaje reenviado -----

De: **Ing. Johana Pedraza** <sistemas@asaludltda.com>

Fecha: 14 de diciembre de 2016, 15:52

Asunto: RE: Servicio Web expuesto en internet Sobre HTTPS - Asalud

Para: Nelsy Angarita <nangarita@colpensiones.gov.co>

Cc: Alberto Barajas Ramon <abarajasr@colpensiones.gov.co>, Arley Fabian Pinzon Vera <afpinzonv@colpensiones.gov.co>

Buenas tardes

Se informa que se realizaron las verificaciones y efectivamente no se encontraban todas las reglas activas en el firewall. Ya están activas y con los bloqueos requeridos. Por favor realizar las pruebas correspondientes, quedamos atentos.

Cordialmente,



Ing. Johana Pedraza

Dir. Tecnología y Sistemas

ASALUD LTDA

Calle 96 # 13a-03 Piso 4

Tel. (1) 2562500 Ext. 110 Celular: 312 451 3065

<http://www.asaludltda.com>

Skype: johana.pedraza

"El contenido de este mensaje electrónico, su texto o elementos adjuntos, son de uso confidencial y privado entre el remitente y su (s) destinatario (s). Cualquier uso o distribución indebida o sin autorización escrita por parte del remitente, se encuentran estrictamente prohibidas y acarrear sanciones penales. Por tanto, en caso de recibir este mensaje por error, por favor notificarlo y devolverlo de inmediato al remitente del mismo, sin guardar copia alguna..."

Por un medio ambiente sano, imprima solo lo necesario.

De: Nelsy Angarita [mailto:nangarita@colpensiones.gov.co]

Enviado el: miércoles, 14 de diciembre de 2016 10:03 a. m.

Para: Ing. Johana Pedraza

CC: Alberto Barajas Ramon

Asunto: Fwd: Servicio Web expuesto en internet Sobre HTTPS - Asalud

Buenos días Johana

Adjunto y en correo precedente envío el reporte de las pruebas de vulnerabilidad realizadas por Colpensiones al servicio de producción expuesto por Asalud para consumo de Colpensiones.

Quedo atenta

----- Mensaje reenviado -----

De: **Alberto Barajas Ramon** <abarajasr@colpensiones.gov.co>

Fecha: 13 de diciembre de 2016, 19:18

Asunto: Re: Servicio Web expuesto en internet Sobre HTTPS - Asalud

Para: Jonathan Forero Tarra <jforerot@colpensiones.gov.co>, Nelsy Angarita

<nangarita@colpensiones.gov.co>, Felipe Eduardo Gallon Medina <fegallonm@colpensiones.gov.co>

Cc: Grupo Comunicaciones <grupo_comunicaciones@colpensiones.gov.co>, Javier Francisco Fúneme Arias <jffunemea@colpensiones.gov.co>, Fredy Alexander Garcia Franco <fagarciaf@colpensiones.gov.co>, Victor Hugo Borrero Angarita <vhborreroa@colpensiones.gov.co>, Liliana Serrano Forero <lserranof@colpensiones.gov.co>

Buen día,

Se adjuntan reportes de las pruebas realizadas, para el día de mañana se envía el consolidado, gracias

- <https://wscolpproduccion.aplicativoasalud.com/INTEGRACIONService/IntegracionService.svc>

Pruebas de Vulnerabilidades generales:

- Reporte: [wscolpproduccion_aplicativoasalud_com_sgk0ja.html](#), Me preocupa que esta expuesto en Internet el Servidor sin control de FW, pues se evidencia múltiples puertos abiertos

Resultado NMAP desde IP Publica (181.205.74.173) Diferente a la de Colpensiones:

Nmap scan report for wscolpproduccion.aplicativoasalud.com (64.37.63.202)

Host is up (0.21s latency).

rDNS record for [64.37.63.202](#): [servidor1.asalud2.com](#)

Not shown: 982 closed ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

21/tcp	open	ftp	Microsoft ftpd
--------	------	-----	----------------

25/tcp	open	smtp	MailEnable smtpd 8.53--
--------	------	------	-------------------------

53/tcp	filtered	domain	
--------	----------	--------	--

80/tcp	open	http	Microsoft IIS httpd 8.5
--------	------	------	-------------------------

110/tcp	open	pop3	MailEnable POP3 Server
---------	------	------	------------------------

135/tcp	open	msrpc	Microsoft Windows RPC
---------	------	-------	-----------------------

139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
---------	------	-------------	-------------------------------

143/tcp	open	imap	MailEnable imapd
---------	------	------	------------------

443/tcp	open	https?	
---------	------	--------	--

445/tcp	open	microsoft-ds	Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
---------	------	--------------	--

3306/tcp	open	mysql	MySQL (unauthorized)
----------	------	-------	----------------------

8443/tcp	open	https-alt?	
----------	------	------------	--

49152/tcp	filtered	unknown	
-----------	----------	---------	--

49153/tcp	open	msrpc	Microsoft Windows RPC
-----------	------	-------	-----------------------

49154/tcp open msrpc Microsoft Windows RPC
49155/tcp open msrpc Microsoft Windows RPC
49156/tcp open msrpc Microsoft Windows RPC
49157/tcp open msrpc Microsoft Windows RPC

Service Info: Host: SERVIDOR1.home; OSs: Windows, Windows Server 2008 R2 - 2012; CPE:
cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 141.43 seconds

Albertos-MacBook-Pro:~ albertobarajas\$ curl ifconfig.co

181.205.74.173

Se adjunta ademas reporte de estado de Certificado y Servicios SSL:

- Clasificado como "B", deben ajustarse temas de algoritmos debiles, "SSL Server Test_
wscolpproduccion.aplicativoasalud_161213_1546.pdf"

Se adjunta reporte de Análisis del WebServices

- Se presentaron alertas de tipo medio, asociadas a mensajes de error, "Developer
Report_Colp_WSAasalud_01_161213.pdf"

- <https://190.25.241.180:9232/COLP.Servicios.ControladorBPM/SvcControladorBPM?wsdl>

Pte para entregar manana.

Saludos cordiales,

**Alberto Barajas Ramón**

Asesor de Vicepresidencia
Vicepresidencia de Operaciones y Tecnología
Carrera 10 N° 72 – 33 Torre B Piso 7º
Teléfono: (57+1) 2170100 Ext. 1516
E-mail: abarajasr@colpensiones.gov.co
<https://www.colpensiones.gov.co>
Bogotá D.C. – Colombia

El 13 de diciembre de 2016, 12:27, Jonathan Forero Tarra <jforerot@colpensiones.gov.co> escribió:

Buen Día,

Agradezco realizar el aseguramiento del consumo del servicio web expuesto por Colpensiones en Internet para que este solo pueda ser accedido por la IP publica de ASALUD **107.161.187.141**, lo anterior a que ya se realizaron las pruebas de vulnerabilidad por parte del grupo de seguridad informática sin presentar novedades, de acuerdo a conversación telefónica con Alberto Barajas.

Por otra parte confirmo la URL de producción donde Asalud expuso el servicio: <https://wscolpproduccion.aplicativoasalud.com/INTEGRACIONService/IntegracionService.svc>

Quedamos atentos al aseguramiento del servicio.

saludos,

El 12 de diciembre de 2016, 20:09, Jonathan Forero Tarra <jforerot@colpensiones.gov.co> escribió:

Buena noche Alberto,

Se realizo la publicación del servicio web en internet Con SSL, el cual sera consumido por Asalud, la URL expuesta del servicio es:

<https://190.25.241.180:9232/COLP.Servicios.ControladorBPM/SvcControladorBPM?wsdl>

Agradezco realizar pruebas de vulnerabilidad a las que hayan lugar o que ustedes consideren.

saludos,

--



Jonathan Forero Tarrá

Profesional Master
Gerencia de Gestión de Sistemas de Información

Vicepresidencia de Operaciones y Tecnología
[Calle 73 No. 10-70](#)

PBX [057] +1 3495444 Ext: 1161

Bogotá D.C. - Colombia
www.colpensiones.gov.co

--



Jonathan Forero Tarrá

Profesional Master
Gerencia de Gestión de Sistemas de Información

Vicepresidencia de Operaciones y Tecnología
[Calle 73 No. 10-70](#)

PBX [057] +1 3495444 Ext: 1161

Bogotá D.C. - Colombia
www.colpensiones.gov.co

--

Nelsy Leonor Angarita Fajardo
Gerencia de Gestion de Sistemas de Informacion

Vicepresidencia de Operaciones y Tecnología
Colpensiones
[Calle 73 No. 10-70](#)

PBX [057] +1 3495444 Ext: 1161

Bogotá D.C. - Colombia
www.colpensiones.gov.co

--



Arley Fabián Pinzón Vera

Profesional

Gerencia Nacional de Reconocimiento

Carrera 7 # 67 - 39 p. 2 Edificio OXO 69

Tel: 2170100 Ext.2565

www.colpensiones.gov.co

Bogotá D.C. - Colombia

--

Nelsy Leonor Angarita Fajardo
Gerencia de Gestion de Sistemas de Informacion
Vicepresidencia de Operaciones y Tecnología
Colpensiones
[Calle 73 No. 10-70](#)
PBX [057] +1 3495444 Ext: 1161
Bogotá D.C. - Colombia
www.colpensiones.gov.co



Arley Fabián Pinzón Vera

Profesional

Gerencia Nacional de Reconocimiento

Carrera 7 # 67 - 39 p. 2 Edificio OXO 69

Tel: 2170100 Ext.2565

www.colpensiones.gov.co

Bogotá D.C. - Colombia



Diana Carolina Cárdenas León

Profesional Master V

Gerencia de Sistemas Integrados de Gestión

[Calle 73 No. 10- 70 Piso 7º](#)

Tel: (57) (1) 2170100 Ext-1401

www.colpensiones.gov.co

Bogotá D.C, Colombia



Arley Fabián Pinzón Vera

Profesional

Dirección de Medicina Laboral

[Carrera 7 # 67 - 39 p. 4 Edificio OXO 69](#)

Ext. 1104

Bogotá D.C. - Colombia

www.colpensiones.gov.co



image001.png
6K