Incidente De Reporte

organizacion	Banvivienda
Fecha	Octubre 13, 2017
Servicio	MSS-VME
Seguridad nivel	Medium
Impacto Nivel	Critical
Vulnerabilidad Nivel	Critical

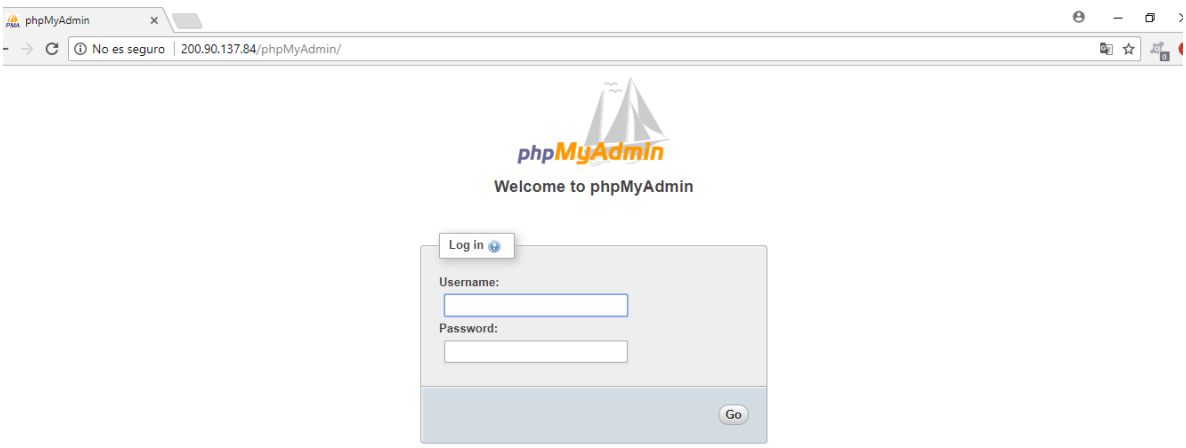
Descripcion

Incidencia de vulnerabilidad de Banvivienda
IP vulnerable: 200.90.137.84, 200.90.137.82
IP cliente Web Server: 200.90.137.84 (pagina web)

El tipo de vulnerabilidad asociado con el servidor web es Web Server Transmits Cleartext Credentials.

En nuestro sistema de monitoreo (GOC) y usando el servicio contratado por ustedes del MSS-VME, detectamos la vulnerabilidad Web Server Transmits Cleartext Credentials en el servidor web que hospeda su sitio principal (www.bancicienda.com) y, haciendo un análisis mayor se detectó que:

1.-) La interfaz web del phpMyAdmin se encuentra instalado en el servidor público del sitio web principal de Banvivienda (www.banvivienda.com) y es **ACCEQUIBLE** desde el URL http://200.90.137.84/phpMyAdmin /. Consideramos en el GOC, esta vulnerabilidad de suma importancia.
2.-) El Web server responde de manera **DISTINTA** si se escribe la URL http://www.banvivienda.com/ o si se escribe http://200.90.137.84/



Data in MSS-VME (logs)

{"vuln_index": 30, "plugin_name": "Web Application Potentially Vulnerable to Clickjacking", "folder_id": 3, "plugin_id": 85582, "uuid": "71aee139-88f3-d6d7-2cf6-fa78d7a8dc964d67eaeb8fa8b22d", "status": "completed", "hostname": "200.90.137.84", "host_start": "Fri Oct 6 11:18:37 2017", "scan_start": 1507306711, "host_id": 20, "scan_type": "local", "hostcount": 9, "sid": "496", "hasaudittrail": true, "plugin_family": "Web Servers", "host_end": "Fri Oct 6 12:47:25 2017", "severity": 2, "timestamp": 1507312050, "count": 1, "user_permissions": 128, "pci-can-upload": false, "scan_end": 1507312050, "scanner_start": 1507306711, "scanner_end": 1507312046, "scanner_name": "Local Scanner", "edit_allowed": true, "haskb": true, "name": "Banvivienda VME", "targets": "200.46.227.224/28,200.46.227.239,200.90.137.80/28,200.90.137.95,200.46.80.104/29,200.46.80.111,200.46.19.96/29,200.46.19.103", "ports": [{"protocol": "www", "port": 80, "transport": "tcp"}], "severity_index": 17, "policy": "GLESEC-GOC", "control": true, "object_id": 496, "host-ip": "200.90.137.84", "operating-system": "Microsoft Windows Vista"}

{"vuln_index": 35, "plugin_name": "Web Server Transmits Cleartext Credentials", "folder_id": 3, "plugin_id": 26194, "uuid": "71aee139-88f3-d6d7-2cf6-fa78d7a8dc964d67eaeb8fa8b22d", "status": "completed", "hostname": "200.90.137.84", "host_start": "Fri Oct 6 11:18:37 2017", "scan_start": 1507306711, "host_id": 20, "scan_type": "local", "hostcount": 9, "sid": "496", "hasaudittrail": true, "plugin_family": "Web Servers", "host_end": "Fri Oct 6 12:47:25 2017", "severity": 1, "timestamp": 1507312050, "count": 1, "user_permissions": 128, "pci-can-upload": false, "scan_end": 1507312050, "scanner_start": 1507306711, "scanner_end": 1507312046, "scanner_name": "Local Scanner", "edit_allowed": true, "haskb": true, "name": "Banvivienda VME", "targets": "200.46.227.224/28,200.46.227.239,200.90.137.80/28,200.90.137.95,200.46.80.104/29,200.46.

80.111,200.46.19.96/29,200.46.19.103", "ports": [{"protocol": "www", "port": 80, "transport": "tcp"}], "severity_index": 16, "policy": "GLESEC-GOC", "control": true, "object_id": 496, "host-ip": "200.90.137.84", "operating-system": "Microsoft Windows Vista"}

{"vuln_index": 29, "plugin_name": "Web Application Potentially Vulnerable to Clickjacking", "folder_id": 3, "plugin_id": 85582, "uuid": "71aee139-88f3-d6d7-2cf6-fa78d7a8dc964d67eaeb8fa8b22d", "status": "completed", "hostname": "200.90.137.82", "host_start": "Fri Oct 6 11:18:36 2017", "scan_start": 1507306711, "host_id": 18, "scan_type": "local", "hostcount": 9, "sid": "496", "hasauditrail": true, "plugin_family": "Web Servers", "host_end": "Fri Oct 6 11:38:43 2017", "severity": 2, "timestamp": 1507312050, "count": 1, "user_permissions": 128, "pci-can-upload": false, "scan_end": 1507312050, "scanner_start": 1507306711, "scanner_end": 1507312046, "scanner_name": "Local Scanner", "edit_allowed": true, "haskb": true, "name": "Banvivienda VME", "targets": "200.46.227.224/28,200.46.227.239,200.90.137.80/28,200.90.137.95,200.46.80.104/29,200.46.80.111,200.46.19.96/29,200.46.19.103", "ports": [{"protocol": "www", "port": 443, "transport": "tcp"}], "severity_index": 16, "policy": "GLESEC-GOC", "control": true, "object_id": 496, "host-ip": "200.90.137.82"}

Web Server Transmits Cleartext Credentials

Descripción

El servidor web remoto contiene varios campos de formulario HTML que contienen una entrada de tipo 'contraseña' que transmiten su información a un servidor web remoto en texto sin cifrar.

Un atacante que espíe el tráfico entre el navegador web y el servidor puede obtener inicios de sesión y contraseñas de usuarios válidos.

Solución

Asegúrese de que todas las formas sensibles transmiten contenido a través de HTTPS.

Systemas Afectados

Ports	**Hosts**
80 / tcp / www	200.90.137.84

Salidas :

Página: / phpmyadmin /

Página de destino: /phpmyadmin/index.php

Página: / phpMyAdmin /

Página de destino: /phpMyAdmin/index.php

Página: /phpmyadmin/index.php

Página de destino: /phpmyadmin/index.php

Página: / phpMyAdmin / index.php
Página de destino: /phpMyAdmin/index.php

Web Application Potentially Vulnerable to Clickjacking
Descripción
El servidor web remoto no establece un encabezado de respuesta X-Frame-Options o un encabezado de respuesta 'antecedentes de trama' de Content-Security-Policy en todas las respuestas de contenido. Esto potencialmente podría exponer el sitio a un ataque por clic o un ataque de reparación de interfaz de usuario, en el que un atacante puede engañar a un usuario para que haga clic en un área de la página vulnerable que sea diferente de lo que el usuario percibe que es la página. Esto puede hacer que un usuario realice transacciones fraudulentas o maliciosas.

X-Frame-Options ha sido propuesta por Microsoft como una forma de mitigar los ataques de clickjacking y actualmente es compatible con todos los principales proveedores de navegadores.

Content-Security-Policy (CSP) ha sido propuesto por el W3C Web Application Security Working Group, con un creciente apoyo entre los principales proveedores de navegadores, como una forma de mitigar clickjacking y otros ataques. La directiva de política 'frame-ancestors' restringe qué fuentes pueden integrar el recurso protegido.

Tenga en cuenta que si bien las cabeceras de respuesta de X-Frame-Options y Content-Security-Policy no son las únicas mitigaciones para el clichacking, actualmente son los métodos más confiables que se pueden detectar mediante la automatización. Por lo tanto, este complemento puede producir falsos positivos si se implementan otras estrategias de mitigación (p. Ej., El marco de busto de JavaScript) o si la página no realiza ninguna transacción sensible a la seguridad.
Solución
Devuelve las opciones X-Frame-Options o Content-Security-Policy (con la directiva "frame-ancestors") con la respuesta de la página.
Esto evita que el contenido de la página se procese por otro sitio cuando se usan las etiquetas HTML de marco o iframe.
Systemas Afectados
80 / tcp / www 200.90.137.84 200.90.137.84

Any questions please let us know.

Sincerely,

GLESEC OPERATION CENTER - GOC