INFORME FINAL DE AUDITORÍA DEL PROGRAMA DE RESULTADOS ELECTORALES PRELIMINARES AGUASCALIENTES 2024 PARA SU PUBLICACIÓN EN SITIO.

- Introducción

El presente documento es el Informe Ejecutivo Final de la Auditoria al Sistema Informático y a la Infraestructura Tecnológica del Programa de Resultados Electorales Preliminares, donde se muestran los resultados obtenidos de las pruebas realizadas durante la Auditoria a la integridad en el procesamiento de la información y la generación de resultados preliminares que se utilizará en la elección local, el día de la jornada electoral.

Estas pruebas permiten conocer el conjunto de condiciones de entrada que ejerciten todos los requisitos funcionales del Programa de Resultados Electorales Preliminares (PREP). En ellas se ignora la estructura de control, concentrándose en los requisitos funcionales del sistema y ejercitándolos. Es decir, se basa en verificar que los datos de entrada plasmados en las Actas de Escrutinio y Cómputo (AEC) sean los que se reflejan en la publicación, Página Web Pública del PREP.

Simultáneamente al proceso de revisión de configuración de infraestructura y pruebas de penetración de la infraestructura del PREP, se realizó un escaneo de vulnerabilidades.

El acceso a los servicios de internet, ha permitido que más personas puedan obtener información para desarrollar ataques en la web. Esto ha generado amenazas entre las que las cibernéticas son un factor importante; por está razón es necesario que los datos contenidos en el PREP tengan una validación de disponibilidad.

La auditoría también tiene como objetivo asegurar la correcta y continua disponibilidad del servicio web de los sitios de publicación de resultados del PREP, durante el período de operación.

- Resumen Ejecutivo

Se utilizaron los equipos instalados por el IEEAgs en los Centros de Acopio y Transmisión de Datos (CATD), y se permitió acceso a los servidores para las pruebas de los módulos de Digitalización, Captura, Verificación, y de Publicación de Resultados.

Posterior a la revisión de los modelos de entrada y salida, fue necesario supervisar en las oficinas del Centro de Captura y Verificación (CCV), los modulos de Captura, Validación y Supervisión.

Las pruebas realizadas consistieron en la ejecución de herramientas informáticas para identificar potenciales vulnerabilidades, y posteriormente en la aplicación de diversas técnicas para intentar explotarlas e identificar así el impacto que tienen sobre la infraestructura y determinar el nivel de exposición de información sensible.

Se evaluó la configuración de los sistemas operativos de los dispositivos que conforman la infraestructura, a través de la comparación con buenas prácticas internacionales de seguridad informática.

El servicio de pruebas de penetración y análisis de vulnerabilidades para la infraestructura tecnológica, tuvo como objeto obtener información relacionada con los activos evaluados, conocer el nivel de exposición de información sensible y documentar los hallazgos.

Finalmente se realizó un ataque de negación de servicio, simulando trafico legitimo y trafico malicioso, semejante al esperado en la jornada electoral, buscando que el servicio de publicación del PREP se mantenga en operación el tiempo requerido.

Como parte de la auditoría se dio seguimiento a los tres simulacros desarrollados en conjunto con el IEEAgs, donde se atestiguó el manejo de las contingencias esperadas.

- Observaciones y Recomendaciones

Se verificó la integridad en el registro de la información por el sistema, es decir: que a partir de un AEC en papel, se genere una imagen digital completa y legible de ésta y sea almacenada sin alteraciones en su contenido y publicada para consulta; **que la imagen digital del AEC, así como sus datos capturados manualmente sean debidamente asociados a la casilla, sección y distrito que corresponda**; que los resultados del AEC capturados sean asociados fielmente al partido, candidatura común, candidatura independiente o rubro en el cual se registren.

Se atendieron los hallazgos de manera satisfactoria para la infraestructura, en materia de configuraciones de infraestructura y, las pruebas de penetración determinaron que **la infraestructura es adecuada para operar en un riesgo bajo**.

Las aplicaciones web no pueden modificarse desde fuera de las instalaciones y el personal del PREP no tiene posibilidades de alterar el contenido de las mismas.

Se determinó que los servidores están protegidos adecuadamente.

Los equipos de telecomunicaciones sólo pueden fallar por desconexión física, pero el

IEEAgs cuenta con, al menos, una conexión de respaldo en cada CATD. Resistieron los ataques internos de negación de servicio.

Se revisaron las instalaciones del CCV y en las mismas se encontró que, a pesar de los ataques, la estaciones de trabajo de todo el personal siguieron trabajando sin problemas.

La página del PREP conservó su continuidad ante el ataque negación de servicio, y fueron bloqueadas al detectarse.

La página, al llegar a los 20GB de promedio **continuó respondiendo adecuadamente ante el tráfico de red**, se iniciaron nuevos ataques a bases de datos y el servicio continuó funcionando.

Por lo que se considera **adecuado para operar el día de la jornada electoral**.

Juriquilla, Querétaro, a 1 de Junio de 2024

Atentamente

M en C Guillermo Vázquez Sánchez
Responsable Técnico

VoBo

Dr. José Luis Aragón Vera
Director del Centro de Física
Aplicada y Tecnología Avanzada

INFORME DE LA APLICACIÓN DE RECOMENDACIONES DE LAS PRUEBAS DE PENETRACIÓN Y REVISIÓN DE CONFIGURACIONES DE LA INFRAESTRUCTURA Y/O SERVICIOS RELACIONADOS CON TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DONDE SE IMPLEMENTE EL PREP AGUASCALIENTES

- Resumen ejecutivo

Las pruebas realizadas consistieron en la ejecución de herramientas informáticas para identificar potenciales vulnerabilidades, y posteriormente en la aplicación de diversas técnicas para intentar explotarlas e identificar así el impacto que tienen sobre la infraestructura y determinar el nivel de exposición de información sensible.

Se evaluó la configuración de los sistemas operativos de los dispositivos que conforman la infraestructura, a través de la comparación con buenas prácticas internacionales de seguridad informática.

La revisión de configuraciones se enfocó en el sistema operativo de servidores, consolas y dispositivos. Así mismo, se verificó la velocidad de las conexiones de internet y que se contara con una conexión de respaldo para el envío de datos.

Todos los hallazgos y oportunidades de mejora que se obtuvieron, como resultado de la ejecución del pentest y de la revisión de configuraciones, se analizaron y se clasificaron.

A partir de los informes de las pruebas de penetración y de la revisión de configuraciones, se verificó la aplicación de las medidas de mitigación aplicadas por el IEEAgs a fin de identificar la persistencia de los hallazgos reportados en la infraestructura de TI.

Utilizando el software Nessus Profesional se realizó un escaneo para establecer los activos sobre los que se realizarán las pruebas y la revisión de configuraciones. Se consideraron los siguientes aspectos: clasificación de los activos por funcionalidad y aspectos técnicos; condiciones de operación actual de los activos a evaluar.

Una vez determinado lo anterior, se designaron los activos primordiales a revisar, se utilizaron además las siguientes herramientas para el pentest: OWASPZAP, Amap, Metasploit, Dmitry, Grabber y SQLmap, hping3, SlowHttpTest.

Para los horarios de pruebas se considero el horario de servicio de CCV y de los CATD.

El servicio de pruebas de penetración y análisis de vulnerabilidades para la infraestructura tecnológica, tuvo como objeto obtener información relacionada con los activos evaluados, conocer el nivel de exposición de información sensible y documentar los hallazgos.

La primera etapa de las pruebas consistió en la identificación de vulnerabilidades en objetivos específicos, así como en otros que podrían proporcionar acceso a información del PREP, intentando explotar las vulnerabilidades identificadas para determinar el impacto potencial en caso de que alguna fuera aprovechada por un usuario malintencionado.

El tiempo de pruebas para cada uno de los activos es limitado, por lo que se definió un plan de pruebas. Entre las vulnerabilidades que trataron de explotarse se encuentran:

1. Instalaciones por defecto.
2. Errores o huecos de seguridad en el software.
3. Configuraciones débiles o vulnerables.
4. Vulnerabilidades que permiten a un atacante remoto acceder de forma no autorizada a información sensible.
5. Vulnerabilidades que permitan a un atacante remoto modificar de forma no autorizada el contenido o la visualización del mismo en un activo de información.
6. Vulnerabilidades que provoquen afectaciones a la disponibilidad de los recursos de TIC.
7. Modificaciones no autorizadas en el contenido de repositorios de documentos (Base de Datos).
8. Verificación de cuentas sin algún tipo de autenticación, cuentas por defecto y contraseñas débiles por medio de ataques de diccionario o fuerza bruta.

Para las pruebas de penetración se consideran dos escenarios: pruebas externas y pruebas internas. En las pruebas externas se evalúan los objetivos que pueden ser alcanzados desde internet y se ejecutan a través de éste mismo medio desde ubicaciones externas a la organización; las pruebas internas incluyen los objetivos que son accesibles sólo desde la red interna y se ejecutan en las instalaciones de la organización.

- Alcance

La revisión de las configuraciones de la infraestructura incluye las visitas a los CATD y la determinación de pruebas de conectividad, en VPNs, Firewalls, etc.
Para la revisión de la infraestructura se revisaron las instalaciones de los 18 CATD Distritales, las instalaciones del CCV, CCV alterno, así como los servidores en la nube.

- Resultado de la Verificación.

Se atendieron los hallazgos de manera satisfactoria para la infraestructura, en materia de configuraciones de infraestructura y, las pruebas de penetración determinaron que la **infraestructura es adecuada para operar en un riesgo bajo**.
Cabe aclarar que esta revisión se basa en clasificación de riesgos, y la auditoria pretende mitigar al máximo los hallazgos que se encontraron. Sin embargo la tecnología avanza rápidamente día con día y nuestra estimación no implica que se llegue a un 0% de riesgo.

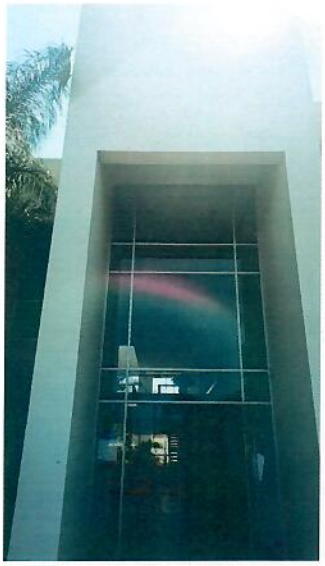
Distrito	Ciudad	CPU	Tablets	Equipamiento	Linea Primaria	Linea 2
I	Rincón de Romos	1	Si	Si	Connectix	MiFi
II	Asientos	1	Si	Si	Connectix	MiFi
III	Pabellón de Arteaga	1	Si	Si	Connectix	MiFi
IV	San Francisco de los Romo	1	Si	Si	Connectix	MiFi
V	Norte	1	Si	Si	Connectix	MiFi
VI	Pocitos	1	Si	Si	Connectix	MiFi
VII	Jesus María	1	Si	Si	Connectix	MiFi
VIII	Calvillo	1	Si	Si	Connectix	MiFi
IX	Pilar Blanco	1	Si	Si	Connectix	MiFi
X	San Nicolas	1	Si	Si	Connectix	MiFi
XI	Centro	1	Si	Si	Connectix	MiFi
XII	Mirador de las Culturas	1	Si	Si	Connectix	MiFi
XIII	Progreso	1	Si	Si	Connectix	MiFi
XIV	Morelos	1	Si	Si	Connectix	MiFi
XV	Ojocaliente	1	Si	Si	Connectix	MiFi
XVI	Valle de los Cactus	1	Si	Si	Connectix	MiFi
XVII	Insurgentes	1	Si	Si	Connectix	MiFi
XVIII	Sur	1	Si	Si	Connectix	MiFi
CCV	Los Cedros	34			Connectix	AcNet
CCVCIDE	CIDE	10			Connectix	

Se había reportado como lista la infraestructura de los CATD el 16 de abril, sin embargo, al ser revisada, se encontró que la misma estaba incompleta o no funcional. Se hizo reporte de hallazgos de cada CATD o CCV, y en cada visita se dio seguimiento hasta verificar las correcciones solicitadas. Los últimos hallazgos fueron atendidos en el simulacro del 23 de Mayo.

No se registró enlace secundario en el CCV CIDE, pues el tipo de conexión requiere de que el personal realice el cambio manualmente en cada una de los equipos, y aunque es funcional, no es eficiente. Por lo que se pidió que dicho cambio sea automático.

El siguiente es un compilado fotográfico de los lugares donde se realizó revisión de infraestructura.


ICTEA
PLANTEL PILAR BLANCO




ICTEA
PLANTEL MIRADOR
DE LAS CULTURAS

Blvd Juriquilla No. 3001, Juriquilla, Qro. C.P 76230
Tel. (55) 5623 4131 y (442) 238 1131.
william@fata.unam.mx

Atentamente

Juriquilla, Querétaro, a 31 de Mayo de 2024

M en C Guillermo Vázquez Sánchez
Responsable Técnico

INFORME FINAL DE LAS PRUEBAS FUNCIONALES DE CAJA NEGRA DEL SISTEMA INFORMÁTICO Y/O SERVICIOS RELACIONADOS CON TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES PREP AGUASCALIENTES 2024

- Introducción

El presente documento tiene como objetivo el evaluar la integridad en el procesamiento de la información y la generación de resultados preliminares que se utilizará en la elección local, el día de la jornada electoral.

Estas pruebas permiten conocer el conjunto de condiciones de entrada que ejerciten todos los requisitos funcionales del Programa de Resultados Electorales Preliminares (PREP). En ellas se ignora la estructura de control, concentrándose en los requisitos funcionales del sistema y ejercitándolos. Es decir, se basa en verificar que los datos de entrada plasmados en las Actas de Escrutinio y Cómputo (AEC) sean los que se reflejan en la publicación, Página Web Pública del PREP.

- Metodología

La revisión se realizó en etapas para analizar el funcionamiento de la aplicación en relación con las fases del proceso técnico operativo, priorizando la digitalización, captura, verificación y publicación de resultados, determinando los flujos completos e interacción entre los diversos módulos. Para el caso del Instituto Estatal Electoral de Aguascalientes (IEEAgs) son: digitalización, validación, captura, verificación, y publicación, debiendo cumplirse cada una de ellas en el orden señalado.

Se utilizaron Casos de Prueba considerando los procesos declarados para cada módulo.

- Criterios utilizados para la auditoría

Los marcados por el Reglamento de Elecciones del Instituto Nacional Electoral y sus Anexos 13 y 18.5. Los Marcados en el procedimiento para Auditorias del la UNAM.

- Resumen Ejecutivo

Se utilizaron los equipos instalados por el IEEAgs en los Centros de Acopio y Transmisión de Datos (CATD), y se permitió acceso a los servidores para las pruebas de los módulos de Digitalización, Captura, Verificación, y de Publicación de Resultados.
Se aplicaron los casos de prueba para cada módulo, las cuales fueron incluidas antes de la prueba funcional.

Posterior a la revisión de los modelos de entrada y salida, fue necesario supervisar en las oficinas del Centro de Captura y Verificación (CCV), los módulos de Digitalización, Captura y Verificación.

Se realizó una segunda prueba funcional para validar los resultados obtenidos, y en ella se reportaron hallazgos y un periodo para su corrección.

- Resultados

El sistema informático permite la captura, digitalización y publicación de los datos asentados en la AEC que se reciben en los CATD.
El sistema informático integra los procesos de captura, validación, transmisión, recepción, consolidación y difusión de los resultados electorales preliminares de las elecciones, en el marco de la normatividad vigente.
El sistema informático apoya las funciones en los CATD, el cual solo incluye la digitalización y transmisión.
El sistema maneja la Integridad en el registro de la información: que a partir de un AEC en papel, se genere una imagen digital completa y legible de ésta y sea almacenada sin alteraciones en su contenido y publicada para consulta; que la imagen digital del AEC, así como sus datos capturados manualmente sean debidamente asociados a la casilla, sección y distrito que corresponda; que los resultados del AEC capturados sean asociados fielmente al partido, coalición, candidatura común o candidato independiente o rubro en el cual se registren.
Para la revisión de desempeño se consideró el universo válido de información de un distrito muestra; únicamente se verificó que el sistema implemente dicha validación o restricción a partir de un catálogo de información el cual deberá tener cargada previamente la información de las casillas válidas. También se consideró la contabilización de actas y presentación de resultados acumulados.

Durante los simulacros se revisó el contenido de todas las paginas, incluyendo ayuntamientos, distritos y secciones. Se marcaron hallazgos durante las revisiones que fueron revisados en simulacros posteriores y, los últimos tres fueron verificados en un simulacro interno el 30 de mayo; donde se marcaron como atendidos.

Por lo que se considera **adecuado para operar**.

Atentamente

Juriquilla, Querétaro, a 1 de Junio de 2024

M en C Guillermo Vázquez Sánchez
Responsable Técnico

INFORME DE RESULTADOS DE LAS PRUEBAS DE NEGACION DE SERVICIO A SITIOS DE PUBLICACIÓN DEL PREP AGUASCALIENTES 2024

- Introducción

El acceso a los servicios de internet, ha permitido que más personas puedan obtener información para desarrollar ataques en la web. Esto ha generado amenazas entre las que las cibernéticas son un factor importante; por está razón es necesario que los datos contenidos en el PREP tengan una validación de disponibilidad.

La auditoría tiene como objetivo asegurar la correcta y continua disponibilidad del servicio web de los sitios de publicación de resultados del PREP, durante el período de operación.

- Pruebas realizadas

Para los ataques se utilizaron las instalaciones del CFATA con la conexión a internet de Telmex, y el servicio de Redwolf. Fungiendo como testigos el personal de Telecomunicaciones del Campus Juriquilla, el personal asignado por el IEEAgs, la empresa encargada de AWS y la empresa Scitum.

Se realizaron ataques en la capa de aplicación (HTTP) con diversos escenarios de SLOWLORIS ATACK como son:

a. Slow headers: consiste en enviar las cabeceras HTTP incompletas (sin el CRLF final que indica el final del header) de tal forma que el servidor no considera las sesiones establecidas y las deja abiertas, afectando al número de conexiones máximas configuradas.
b. Range (Apache killer): se crean numerosas peticiones superponiendo rangos de bytes en la cabecera (HTTP ranges), agotando los recursos de memoria y CPU del servidor.
c. Slow read: en este caso se envían peticiones HTTP legítimas, pero se ralentiza el proceso de lectura de la respuesta, retrasando el envío de ACK (HTTP es TCP).

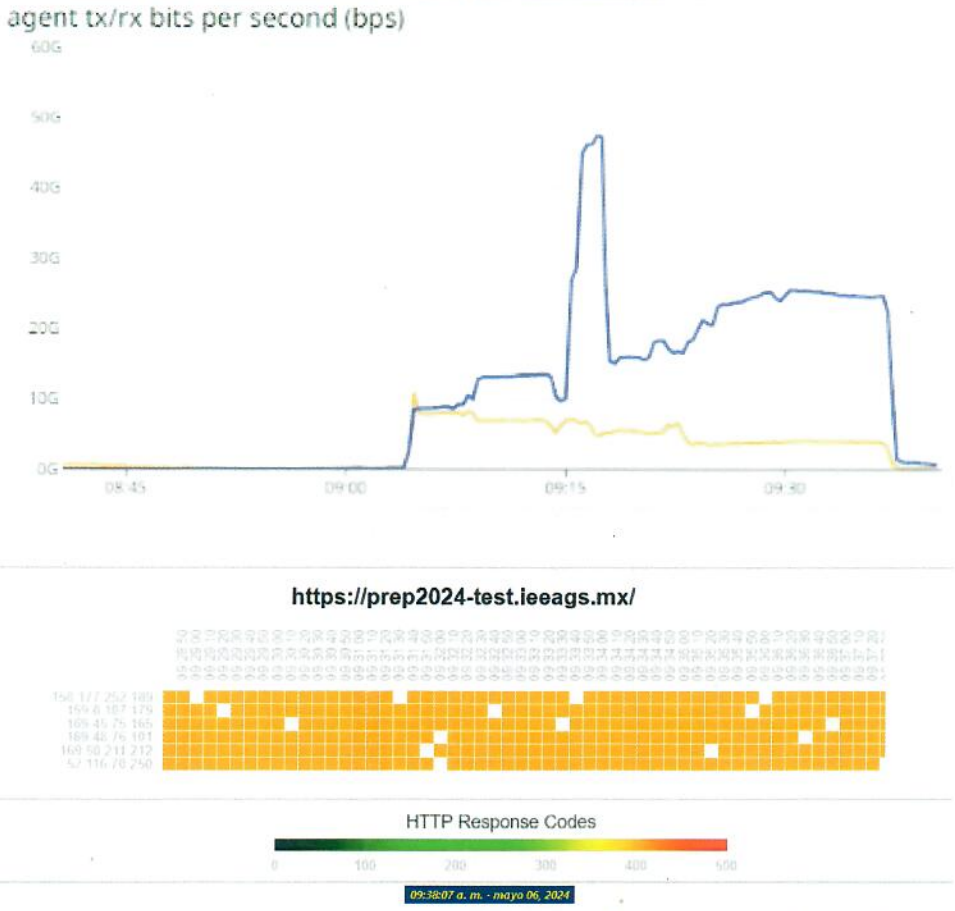
Se realizaron ataques volumétricos con los vectores DNS QUERY FLOOD, SLOWLORIS ATTACK, CACHE-BUSTING Y HTTP. Adicionalmente se incluyeron por los protocolos TCP (con SYN FLOOD), UDP (con DNS Amplification), ICMP con (ICMP Flood), empleando IP aleatorias, para que no se identificara el atacante. Al mismo tiempo se simuló trafico no malintencionado con el que se simuló tráfico legitimo.

Se analizaron dos veces los servidores prep2024-test.ieeags.mx y, para el ataque slowloris, se inició con la página de diputaciones, el cual fue previamente escaneado para obtener sus vulnerabilidades y explotarlas durante el ataque.

- Resultados

1. El escaneo no proporcionó información de vulnerabilidades de alto riesgo.
2. El servicio conservó su continuidad ante el ataque de slowloris, y en algunos casos fueron bloqueadas al detectarse.
3. **La página, al llegar a los** 25GB de promedio **continuó respondiendo adecuadamente ante el tráfico de red**, se iniciaron nuevos ataques a bases de datos y el servicio continuó funcionando.

Se muestran las gráficas de resultados del ataque volumétrico.



Atentamente

Juriquilla, Querétaro, a 31 de Mayo de 2024

M en C Guillermo Vázquez Sánchez
Responsable Técnico

INFORME FINAL DE ANÁLISIS DE VULNERABILIDADES A LA INFRAESTRUCTURA Y/O SERVICIOS RELACIONADOS CON TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DONDE SE IMPLEMENTE EL PREP AGUASCALIENTES.

- Introducción

Simultáneamente al proceso de revisión de configuración de infraestructura y pruebas de penetración de la infraestructura del PREP, se realizó un escaneo de vulnerabilidades. Una vez identificados los puntos de vulnerabilidades, el análisis se enfocó primordialmente en servidores, aplicaciones web, equipos de telecomunicaciones y estaciones de trabajo (estos últimos en el CCV).

Una vez determinado los activos a analizar, se utilizaron además las siguientes herramientas para el pentest: OWASPZAP, Amap, Metasploit, Dmitry, Grabber y SQLmap, hping3, SlowHttpTest. Se realizaron ataques desde el interior y el exterior tratando de cambiar los datos en el AEC, los datos de la Base de Datos o inutilizar los equipos para que no se pudiera realizar alguno de los procesos del PREP.

- Resultados Generales

Se determinó que los servidores están protegidos adecuadamente.

Las aplicaciones web no pueden modificarse desde fuera de las instalaciones y el personal del PREP no tiene posibilidades de alterar el contenido de las mismas.

Los equipos de telecomunicaciones sólo pueden fallar por desconexión física, pero el IEEAgs cuenta con, al menos, una conexión de respaldo en cada CATD. Resistieron los ataques internos de negación de servicio.

Se revisaron las instalaciones del CCV y en las mismas se encontró que, a pesar de los ataques, la estaciones de trabajo de todo el personal siguieron trabajando sin problemas.

Para cada instalación se generó un reporte como el que se muestra enseguida y solo se entregaron al IEEAgs aquellos que eran necesario mitigar. No se presentaron riesgos en los CATD.

Todos los hallazgos fueron atendidos y revisados a mas tardar el 30 de mayo. Las recomendaciones de buenas practicas se revisaron igualmente en toda la infraestructura.

En el CCV Harris se encontró un equipo con una vulnerabilidad, y para mitigarla se decidió remover el equipo de la sede para que no representara riesgo.

XXX.XX.X.1

Crítico	Alto	Medio	Bajo	Información
1	4	10	4	27

Vulnerabilities

106608 - OpenSSH 5.4 < 7.1p2 Multiple Vulnerabilities -

Synopsis
The SSH server running on the remote host is affected by multiple vulnerabilities.

Description
According to its banner, the version of OpenSSH running on the remote host is 5.x prior to 5.4, 6.x or 7.x prior to 7.1p2. It is, therefore, affected by multiple vulnerabilities.

- A potential information disclosure vulnerability which may allow remote servers to obtain sensitive information from process memory by requesting transmission of an entire buffer (CVE-2016-0777)

- A denial of service vulnerability due to a heap-base overflow in roaming_common.c (CVE-2016-0778)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution
Upgrade to OpenSSH version 7.1p2 or later.

Risk Factor
High

CVSS Base Score
CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Plugin Information
Published: 2/5/2018, Modified: 3/27/2024

Atentamente

Juriquilla, Querétaro, a 31 de Mayo de 2024

M en C Guillermo Vázquez Sánchez
Responsable Técnico