GRUPO HORUS

Asunción, 13 de junio de 2023

Señor
Richard Fabian Baddouh Berni, Coordinador TIC de la Unidad Ejecutora de Programas y Proyectos del Ministerio de Educación y Ciencias
Ministerio de Educación y Ciencias (MEC)

REF.: Entrega del Producto 3 "**Informe de Seguridad de los Sistemas**" conforme Orden de Inicio de Servicios en el marco del contrato N°07-22 CD – Contratación Directa Nº 01/2022 "CONSULTORIA PARA EL DIAGNOSTICO Y EVALUACIÓN DE LA SEGURIDAD DE LOS SISTEMAS TRANSACCIONALES DEL MEC (HACKING ETICO) - SEGUNDO LLAMADO"ID: 416.862.

Presente

De nuestra mayor consideración,

Tenemos el agrado de dirigirnos a Usted en el marco del *contrato N°07-22 CD – Contratación Directa Nº 01/2022 "CONSULTORIA PARA EL DIAGNOSTICO Y EVALUACIÓN DE LA SEGURIDAD DE LOS SISTEMAS TRANSACCIONALES DEL MEC (HACKING ETICO) - SEGUNDO LLAMADO"ID: 416.862. Para realizar la entrega del siguiente Producto:*

- *Producto 3: 1(un) Informe Ejecutivo de Seguridad, hallazgos y evidencias de las vulnerabilidades de los sistemas transaccionales de gestión e información del MEC, incluyendo recomendaciones concretas que permitan corregir los problemas y brechas de seguridad. Así mismo, este informe dispone de dos documentos con contenido confidencial los mismos se encuentran alojados en un sharepoint proveído por el MEC*:

1. MEC ANALISIS_EXTERNO_002
2. MEC ANALISIS_INTERNO_003

Aprovechamos la oportunidad para saludarlos muy atentamente.

George Temperley Ovalle
Representante Legal
GRUPO HORUS S.A.
GRUPO HORUS
GRUPO HORUS S.A.

TIC - C
Exp. Nº
Recibido por: Fabiana
Día | Mes | Año | Hora
13 | 06 | 2023 | 11:00hs.

Avda. Brasilia 228 • CP 1208 • Asunción, Paraguay
+595 21 606 320
www.grupohorus.com.py
info@horustek.com

EVALUACIÓN DE CIBERSEGURIDAD

INFORME
PRODUCTO 3

CONSULTORÍA PARA EL DIAGNÓSTICO Y EVALUACIÓN DE LA SEGURIDAD DE LOS SISTEMAS TRANSACCIONALES DEL MEC" (HACKING ÉTICO)

GRUPO HORUS
GRUPO HORUS S.A.

Código	MEC_002
Versión	**0.1**
Fecha de la versión	13-06-2023
Creado	Grupo Horus
Aprobado por	
Nivel de confidencialidad	CONFIDENCIAL

Histórico de Versiones

Fecha	Versión	Modificación	Realizado por
...	1.0	Versión Aprobada	
	1.1		
	1.2		

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el MEC. Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS

GRUPO HORUS S.R.

Tabla de contenido

Glosario 3

Antecedentes 4

RECOMENDACIONES 7

A. XXX - ANONIMIZADO 7

B. XXX - ANONIMIZADO 9

C. XXX - ANONIMIZADO 11

D. SITE-WEB 12

E. XXX - ANONIMIZADO 13

F. XXX - ANONIMIZADO 14

G. Datos 15

H. XXX - ANONIMIZADO 16

I. XXX - ANONIMIZADO 17

J. XXX - ANONIMIZADO 18

K. MEC 18

1. Default Tomcat User and Password (apache-tomcat-default-password) 22
2. Postgres default account: postgres/no password 22
3. Samba RPC unauthenticated remote code execution (CVE-2012-1182) 22
4. PHP Vulnerability: CVE-2015-0235 23
5. Apache Tomcat: Important: Remote Code Execution on Windows (CVE-2019-0232) 23
6. Webmin: Unauthenticated Remote Code Execution 23
7. PostgreSQL class A vulnerability in core server: CVE-2013-1899 23
8. HTTP TRACE Method Enabled 24
9. Apache Tomcat: Important: Remote Code Execution (CVE-2017-12617) 24
10. Default SSH password: admin password "admin" 24

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el MEC. Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS

GRUPO HORUS S.A.

1. Glosario

- **Amenaza:** Acción o evento que puede comprometer la seguridad. Es una potencial violación a la seguridad.
- **Vulnerabilidad:** Existencia de debilidad, diseño o implementación de un error que puede desencadenar un evento comprometedor.
- **Blanco de evaluación:** Sistema, producto o componente que es identificado/sometido y que requiere de evaluación de seguridad.
- **Ataque:** Es un asalto a la seguridad del sistema y que es derivado de una amenaza inteligente. Un ataque es cualquier acción que viole la seguridad.
- **Explotación:** Es un método definido que viola la seguridad de un sistema informático a través de una vulnerabilidad.
- **DDoS**: En seguridad informática, un ataque de denegación de servicios, también llamado ataque DoS (de las siglas en inglés Denial of Service) o DDoS (de Distributed Denial of Service), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.
- **Fuerza Bruta**: En criptografía, se denomina ataque de fuerza bruta a la forma de recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso.
- **XSS**: del inglés Cross-site scripting es un tipo de inseguridad informática o agujero de seguridad típico de las aplicaciones Web, que permite a una tercera persona inyectar en páginas web visitadas por el usuario código JavaScript o en otro lenguaje similar.
- **XXX - ANONIMIZADO**: Servicio, dirección URL o aplicación web anonimizado por seguridad.

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el MEC. Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS
GRUPO HORUS S.A.

2. Antecedentes

La Consultoría fue realizada por un equipo de profesionales multidisciplinarios, quienes poseen conocimiento, entrenamiento y experiencia probadas en el ámbito de las TIC.

Este documento tiene como objetivo mostrar los trabajos realizados en el marco del producto 3, el mismo contiene un resumen de las recomendaciones dadas a la institución para corregir los problemas y brechas de seguridad detectados y mitigar los riesgos asociados a los sistemas de la Institución.

Debido a la alta confidencialidad de los trabajos y datos recogidos, el contenido en extenso del trabajo será depositado en un repositorio especial proveído por el MEC, a modo de que estos datos puedan estar protegidos de cualquier eventualidad.

Cabe resaltar que el ANÁLISIS DE VULNERABILIDADES fue autorizado por MEC, a fin de determinar la vulnerabilidad y posibles cursos de acción para mitigar los mismos.

El trabajo ejecutado consiste en que el beneficiario no proporciona información sobre la estructura de sus redes o las características de sus sistemas. Es el equipo de consultores que realiza la auditoría la que obtiene esta información. De esta forma el servicio son objetivos y siguen los mismos pasos que un atacante que estuviese intentando vulnerar los sistemas de la institución.

Observación

En base a las vulnerabilidades encontradas, se procedió a realizar la valoración del riesgo asociado a cada vulnerabilidad y a partir de la misma se obtuvo la lista de las principales vulnerabilidades que representan un mayor riesgo a efectos de ciberseguridad.

Nota: A efectos de mejor identificación en lo repositorio de ciberseguridad (CVE – CWE, Bugtrack, etc) se mantiene el título de la vulnerabilidad en inglés.

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el MEC. Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

3. Objetivos

3.1 **Identificar Vulnerabilidades:** El objetivo principal de un test de seguridad es identificar y documentar las vulnerabilidades de seguridad en un sistema, red, aplicación u organización. Esto incluye tanto vulnerabilidades conocidas (debilidades comunes) como vulnerabilidades desconocidas (debilidades previamente no descubiertas).

Evaluar los Controles de Seguridad: El test de seguridad es evalúa la eficacia de los controles de seguridad y las medidas implementadas. Esto ayuda a las organizaciones a comprender si sus medidas de seguridad son suficientes para protegerse contra posibles amenazas.

Medir la Resiliencia de la Seguridad: Al simular escenarios de ataque del mundo real, la prueba de penetración evalúa cuán bien una organización puede resistir y recuperarse de incidentes de seguridad. Esto proporciona una visión de la postura de seguridad general de una organización.

Verificación de Cumplimiento: En muchas industrias y organismos reguladores se requieren pruebas de seguridad periódicas para garantizar el cumplimiento de estándares y regulaciones de seguridad. Los test de seguridad ayudan a las organizaciones a demostrar su compromiso con la seguridad y el cumplimiento.

Gestión de Riesgos: ayudan a las organizaciones a identificar y priorizar los riesgos de seguridad. Al comprender estos riesgos, las organizaciones pueden tomar decisiones informadas sobre la asignación de recursos para mejoras de seguridad.

Concienciación sobre la Seguridad: Las pruebas de penetración pueden crear conciencia entre el personal de una organización sobre la importancia de la seguridad. Ayudan a los empleados a reconocer las posibles amenazas y vulnerabilidades sobre las que deben estar atentos.

4. Actividades desarrolladas

Se ha realizado tareas para hallar las vulnerabilidades en los sistemas transaccionales de gestión e información del MEC, para lo cual se ha hecho un Análisis de Vulnerabilidades Externas, es decir, un análisis de las vulnerabilidades que podrían ser explotables por un atacante ubicado en Internet.

El Análisis de Vulnerabilidades Externa se realizó a: A los sistemas del MEC publicados a internet que fueron identificados por la dirección de Tecnología del MEC.

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el MEC. Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS
GRUPO HORUS S.A.

Las tareas realizadas bajo la denominación de:

4.1 Caja negra: sin usuarios ni información previa.

4.2. Caja gris: sin usuarios, pero contando con el detalle de las aplicaciones y de la infraestructura perimetral de la organización.

4.3. Caja blanca: contando con los usuarios de aplicación o de sistemas suficientes para acceder de manera directa (proveído por el MEC).

Las tareas realizadas incluyeron sitios como:

Nombre	**Servicio**
SITIO WEB	https://XXX - ANONIMIZADO.mec.gov.py/
SITIO WEB	https://XXX - ANONIMIZADO.mec.gov.py/
SITIO WEB	https://XXX - ANONIMIZADO.mec.gov.py/XXX - ANONIMIZADO
SITIO WEB	https://XXX - ANONIMIZADO.mec.gov.py/
SITIO WEB	https://XXX - ANONIMIZADO.mec.gov.py/
SITIO WEB	https://XXX - ANONIMIZADO.mec.gov.py/
SITIO WEB	https://XXX - ANONIMIZADO.gov.py/
SITIO WEB	https://XXX - ANONIMIZADOescolar.mec.gov.py/
SITIO WEB	https://XXX - ANONIMIZADO.mec.gov.py/
SITIO WEB	https://XXX - ANONIMIZADO.mec.edu.py/
SITIO WEB	https://.gov.py/cms/

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el MEC. Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS

GRUPO HORUS S.A.

5. Recomendaciones para Sitios Externos

Es importante implementar **Content Security Policy** (CSP) en los sitios web por varias razones fundamentales:

Mitigación de Ataques XSS: CSP es una medida efectiva para mitigar ataques de Cross-Site Scripting (XSS), que son una de las amenazas de seguridad más comunes en la web. Al definir una política CSP, puedes especificar de dónde se pueden cargar scripts en tu sitio web. Esto limita la capacidad de un atacante para inyectar código malicioso en tus páginas a través de vulnerabilidades XSS.

Reducción de Riesgos de Clickjacking: CSP también ayuda a prevenir ataques de clickjacking, donde los atacantes ocultan contenido malicioso detrás de elementos en un sitio web legítimo. Con CSP, puedes indicar quién tiene permiso para embeber tu sitio web en un marco (frame), evitando que terceros lo incluyan en un marco malicioso.

Mejora de la Seguridad General: CSP proporciona un mecanismo para reforzar la seguridad general de un sitio web. Limita la ejecución de código no autorizado y ayuda a prevenir la exposición de datos sensibles o la ejecución de acciones no deseadas en un sitio web.

Protección de la Privacidad del Usuario: CSP también puede ayudar a proteger la privacidad de los usuarios al limitar el acceso a ciertos recursos, como cámaras y micrófonos, lo que evita el acceso no autorizado a dispositivos del usuario.

Prevención de Cargas Maliciosas: CSP puede ayudar a evitar la carga de recursos maliciosos o no deseados desde dominios externos. Esto es particularmente útil para prevenir la inyección de publicidad maliciosa o la carga de scripts de terceros no confiables.

Facilita la Identificación de Problemas de Seguridad: La implementación de CSP puede ayudar a identificar y diagnosticar problemas de seguridad en un sitio web. Los informes de violaciones de política CSP proporcionan información valiosa sobre intentos de ataque y vulnerabilidades potenciales.

Cumplimiento de Estándares de Seguridad: En ciertos entornos, como aplicaciones financiera o gubernamentales, la implementación de CSP puede ser un requisito para cumplir con estándares y regulaciones de seguridad.

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el MEC. Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS

A. XXX - ANONIMIZADO –

https://XXX - ANONIMIZADO.mec.gov.py/XXX - ANONIMIZADO/

1. Vulnerabilidad	**Clickjacking**: es un ataque basado en la interfaz que engaña a los usuarios de un sitio web para que sin saberlo hagan clic en enlaces maliciosos. En clickjacking, los atacantes incrustan sus enlaces maliciosos en botones o páginas legítimas en un sitio web
Recomendaciones	
X-FRAME-OPTIONS	El encabezado X-Frame-Option permite tres valores. ● DENY, que prohíbe mostrar la página dentro de un marco ● SAMEORIGIN, que permite mostrar la página dentro de un marco, siempre que permanezca en el mismo dominio ● PERMITIR-DESDE URI, que permite la visualización de la página dentro de un marco, pero solo en un URI específico (identificador uniforme de recursos), por ejemplo, solo dentro de una página web específica en particular.
Para prevenir los ataques de clickjacking es pedir al navegador que bloquee cualquier intento de cargar tu sitio web dentro de un iframe. Puedes hacerlo enviando la cabecera HTTP X-Frame-Options. El encabezado proporciona al propietario del sitio web control sobre el uso de iframes u objetos, de modo que la inclusión de una página web dentro de un marco/frame puede prohibirse con la directiva deny: **X-Frame-Options: deny**	
2. Vulnerabilidad	**Web Server Information Disclosure**: La aplicación de destino revela la versión del software del servidor web a través del token "Servidor:" enviado en el encabezado de respuesta HTTP.
Recomendaciones	
Content Security Policy	Los contenidos activos en páginas web, como por ejemplo JavaScript, CSS o ActiveX, plantean riesgos de seguridad para los usuarios de Internet y los gestores de páginas web y pueden manipularse. Para que las páginas de Internet puedan utilizarse sin preocupaciones, existe lo que se conoce como Content Security Policy (CSP), cuyo papel consiste en proteger a las páginas frente a ataques perjudiciales y es compatible con la mayoría de navegadores web.
Ejemplos de CSP: 1. script-src "https://example.com:443" – Solo se permiten scripts de este dominio por HTTPS. 2. script-src 'none' – No se pueden cargar scripts. 3. script-src 'self' – Solo pueden cargarse scripts que tengan el mismo origen que la página actual, pero no el de los subdominios. 4. script-src https: – Se pueden cargar scripts de cualquier dominio siempre que empiecen por HTTPS. 5. script-src example.com – Se pueden cargar scripts de este dominio. 6. script-src *.example.com – Se permiten scripts de este y de todos los dominios. 7. img-src data: – Pueden cargarse imágenes por medio de enlaces de datos.	
3. Vulnerabilidad	**Apache HTTP Server Buffer Overflow Vulnerability**: Apache HTTP Server, coloquialmente llamado Apache, es un software de servidor web multiplataforma gratuito y de código abierto.

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el MEC. Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS

	En las versiones afectadas de Apache HTTP Server, un envío de solicitud cuidadosamente elaborado puede provocar un desbordamiento de búfer ocasionando una denegación de servicio.
Recomendaciones	
Update Apache	Se recomienda a los clientes que actualicen a Apache HTTP Server (version actualizada 2.4.57) a una versión posterior para remediar esta vulnerabilidad.
Instalar Actualizar apache server	
4. Vulnerabilidad	**Use of JavaScript Library with Known Vulnerability**: La aplicación web utiliza una biblioteca de JavaScript que se sabe que contiene al menos una vulnerabilidad.
Recomendaciones	
Update Librerías	Se recomienda la actualización de las dependencias y librerías instaladas.
Debe existir un proceso de administración de parches para: • Eliminar las dependencias no utilizadas, las funciones, los componentes, los archivos y la documentación innecesarios. • Haga un inventario continuo de las versiones de los componentes del lado del cliente y del lado del servidor (por ejemplo, marcos, bibliotecas) y sus dependencias utilizando herramientas como versiones, OWASP Dependency Check, retire.js, etc. Monitoree continuamente fuentes como Common Vulnerability and Exposures (CVE) y National Vulnerability Database (NVD) para detectar vulnerabilidades en los componentes. • Solo obtenga componentes de fuentes oficiales a través de enlaces seguros. Prefiera los paquetes firmados para reducir la posibilidad de incluir un componente malicioso modificado. • Supervise las bibliotecas y los componentes que no reciben mantenimiento o que no crean parches de seguridad para versiones anteriores. Si no es posible aplicar parches, considere implementar un parche virtual para monitorear, detectar o proteger contra el problema descubierto. • Cada organización debe garantizar un plan continuo para monitorear, clasificar y aplicar actualizaciones o cambios de configuración durante la vida útil de la aplicación o cartera.	

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el MEC. Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS

GRUPO HORUS S.A.

B. XXX - ANONIMIZADO

https://XXX - ANONIMIZADO.mec.gov.py/XXX - ANONIMIZADO/

1. Vulnerabilidad	**Clickjacking**: es un ataque basado en la interfaz que engaña a los usuarios de un sitio web para que sin saberlo hagan clic en enlaces maliciosos. En clickjacking, los atacantes incrustan sus enlaces maliciosos en botones o páginas legítimas en un sitio web
Recomendaciones	
X-FRAME-OPTIONS	El encabezado X-Frame-Option permite tres valores. • DENY, que prohibe mostrar la página dentro de un marco • SAMEORIGIN, que permite mostrar la página dentro de un marco, siempre que permanezca en el mismo dominio • PERMITIR-DESDE URI, que permite la visualización de la página dentro de un marco, pero solo en un URI específico (Identificador uniforme de recursos), por ejemplo, solo dentro de una página web específica en particular.
Para prevenir los ataques de clickjacking es pedir al navegador que bloquee cualquier intento de cargar tu sitio web dentro de un iframe. Puedes hacerlo enviando la cabecera HTTP X-Frame-Options. El encabezado proporciona al propietario del sitio web control sobre el uso de iframes u objetos, de modo que la inclusión de una página web dentro de un marco/frame puede prohibirse con la directiva deny: **X-Frame-Options: deny**	
2. Vulnerabilidad	**Vulnerabilidad basada en rutas**: se descubrió un archivo, directorio o lista de directorios potencialmente confidencial en el servidor web.
Recomendaciones	
Path Disclosure	Las vulnerabilidades de divulgación de ruta completa (FPD) permiten al atacante ver la ruta al archivo/raíz web. por ejemplo: /inicio/omg/htdocs/archivo/. Ciertas vulnerabilidades, como el uso de la consulta load_file() (dentro de una inyección SQL) para ver el código fuente de la página, requieren que el atacante tenga la ruta completa al archivo que desea ver.

La forma de proteger su servidor web de los ataques de divulgación de ruta completa es editando el archivo php.ini de su servidor para:
 	
Deshabilitar el informe de errores:
error_reporting(0);
Ocultar mensajes de error:
display_errors(0);	

3. Vulnerabilidad	**Use of JavaScript Library with Known Vulnerability:** La aplicación web utiliza una biblioteca de JavaScript que se sabe que contiene al menos una vulnerabilidad.
Recomendaciones	

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el MEC. Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS

GRUPO HORUS S.A.

Update Librerías	Se recomienda la actualización de las dependencias y librerías instaladas.

Debe existir un proceso de administración de parches para:

- Eliminar las dependencias no utilizadas, las funciones, los componentes, los archivos y la documentación innecesarios.
- Haga un inventario continuo de las versiones de los componentes del lado del cliente y del lado del servidor (por ejemplo, marcos, bibliotecas) y sus dependencias utilizando herramientas como versiones, OWASP Dependency Check, retire.js, etc. Monitoree continuamente fuentes como Common Vulnerability and Exposures (CVE) y National Vulnerability Database (NVD) para detectar vulnerabilidades en los componentes.
- Solo obtenga componentes de fuentes oficiales a través de enlaces seguros. Prefiera los paquetes firmados para reducir la posibilidad de incluir un componente malicioso modificado.
- Supervise las bibliotecas y los componentes que no reciben mantenimiento o que no crean parches de seguridad para versiones anteriores. Si no es posible aplicar parches, considere implementar un parche virtual para monitorear, detectar o proteger contra el problema descubierto.
- Cada organización debe garantizar un plan continuo para monitorear, clasificar y aplicar actualizaciones o cambios de configuración durante la vida útil de la aplicación o cartera.

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el MEC. Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS

GRUPO HORUS S.A.

C. XXX - ANONIMIZADO - XXX - ANONIMIZADO

https://XXX - ANONIMIZADO.mec.gov.py/XXX - ANONIMIZADO

1. Vulnerabilidad	**Clickjacking**: es un ataque basado en la interfaz que engaña a los usuarios de un sitio web para que sin saberlo hagan clic en enlaces maliciosos. En clickjacking, los atacantes incrustan sus enlaces maliciosos en botones o páginas legítimas en un sitio web
Recomendaciones	
X-FRAME-OPTIONS	El encabezado X-Frame-Option permite tres valores. • DENY, que prohíbe mostrar la página dentro de un marco • SAMEORIGIN, que permite mostrar la página dentro de un marco, siempre que permanezca en el mismo dominio • PERMITIR-DESDE URI, que permite la visualización de la página dentro de un marco, pero solo en un URI específico (Identificador uniforme de recursos), por ejemplo, solo dentro de una página web específica en particular.
Para prevenir los ataques de clickjacking es pedir al navegador que bloquee cualquier intento de cargar tu sitio web dentro de un iframe. Puedes hacerlo enviando la cabecera HTTP X-Frame-Options. El encabezado proporciona al propietario del sitio web control sobre el uso de iframes u objetos, de modo que la inclusión de una página web dentro de un marco/frame puede prohibirse con la directiva deny: **X-Frame-Options: deny**	
2. Vulnerabilidad	**Vulnerabilidad basada en rutas:** se descubrió un archivo, directorio o lista de directorios potencialmente confidencial en el servidor web.
Recomendaciones	
Path Disclosure	Las vulnerabilidades de divulgación de ruta completa (FPD) permiten al atacante ver la ruta al archivo/raíz web. por ejemplo: /inicio/omg/htdocs/archivo/. Ciertas vulnerabilidades, como el uso de la consulta load_file() (dentro de una inyección SQL) para ver el código fuente de la página, requieren que el atacante tenga la ruta completa al archivo que desea ver.

La forma de proteger su servidor web de los ataques de divulgación de ruta completa es editando el archivo php.ini de su servidor para:
 	
Deshabilitar el informe de errores:
error_reporting(0);
Ocultar mensajes de error:
display_errors(0);	

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el MEC. Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS

GRUPO HORUS S.A.

D. SITE-WEB

https://XXX - ANONIMIZADO.mec.gov.py/

1. Vulnerabilidad	**Vulnerabilidad basada en rutas:** se descubrió un archivo, directorio o lista de directorios potencialmente confidencial en el servidor web.
Recomendaciones	
Path Disclosure	Las vulnerabilidades de divulgación de ruta completa (FPD) permiten al atacante ver la ruta al archivo/raíz web. por ejemplo: /inicio/omg/htdocs/archivo/. Ciertas vulnerabilidades, como el uso de la consulta load_file() (dentro de una inyección SQL) para ver el código fuente de la página, requieren que el atacante tenga la ruta completa al archivo que desea ver.

La forma de proteger su servidor web de los ataques de divulgación de ruta completa es editando el archivo php.ini de su servidor para:
 	
Deshabilitar el informe de errores:
error_reporting(0);
Ocultar mensajes de error:
display_errors(0);	

2. Vulnerabilidad	**Apache HTTP Server Buffer Overflow Vulnerability:** Apache HTTP Server, coloquialmente llamado Apache, es un software de servidor web multiplataforma gratuito y de código abierto. En las versiones afectadas de Apache HTTP Server, un envío de solicitud cuidadosamente elaborado puede provocar un desbordamiento de búfer ocasionando una denegación de servicio.
Recomendaciones	
Update Apache	Se recomienda a los clientes que actualicen a Apache HTTP Server (versión actualizada 2.4.57) a una versión posterior para remediar esta vulnerabilidad.
Instalar, actualizar Apache Server	

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el MEC. Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS

GRUPO HORUS S.A.

E. XXX - ANONIMIZADO

https://XXX - ANONIMIZADO.mec.gov.py

1. Vulnerabilidad	**Vulnerabilidad basada en rutas:** se descubrió un archivo, directorio o lista de directorios potencialmente confidencial en el servidor web.
Recomendaciones	
Path Disclosure	Las vulnerabilidades de divulgación de ruta completa (FPD) permiten al atacante ver la ruta al archivo/raíz web. por ejemplo: /inicio/omg/htdocs/archivo/. Ciertas vulnerabilidades, como el uso de la consulta load_file() (dentro de una inyección SQL) para ver el código fuente de la página, requieren que el atacante tenga la ruta completa al archivo que desea ver.

La forma de proteger su servidor web de los ataques de divulgación de ruta completa es editando el archivo php.ini de su servidor para:
 	
Deshabilitar el informe de errores:
error_reporting(0);
Ocultar mensajes de error:
display_errors(0);	

2. Vulnerabilidad	**Apache HTTP Server Buffer Overflow Vulnerability:** Apache HTTP Server, coloquialmente llamado Apache, es un software de servidor web multiplataforma gratuito y de código abierto. En las versiones afectadas de Apache HTTP Server, un envío de solicitud cuidadosamente elaborado puede provocar un desbordamiento de búfer ocasionando una denegación de servicio.
Recomendaciones	
Update Apache	Se recomienda a los clientes que actualicen a Apache HTTP Server (versión actualizada 2.4.57) a una versión posterior para remediar esta vulnerabilidad.
Instalar, actualizar Apache Server	

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el MEC. Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS

GRUPO HORUS S.A.

F. XXX - ANONIMIZADO

https://XXX - ANONIMIZADO.mec.gov.py/

1. Vulnerabilidad	**Clickjacking**: es un ataque basado en la interfaz que engaña a los usuarios de un sitio web para que sin saberlo hagan clic en enlaces maliciosos. En clickjacking, los atacantes incrustan sus enlaces maliciosos en botones o páginas legítimas en un sitio web
Recomendaciones	
X-FRAME-OPTIONS	El encabezado X-Frame-Option permite tres valores. • DENY, que prohíbe mostrar la página dentro de un marco • SAMEORIGIN, que permite mostrar la página dentro de un marco, siempre que permanezca en el mismo dominio • PERMITIR-DESDE URI, que permite la visualización de la página dentro de un marco, pero solo en un URI específico (Identificador uniforme de recursos), por ejemplo, solo dentro de una página web específica en particular.
Para prevenir los ataques de clickjacking es pedir al navegador que bloquee cualquier intento de cargar tu sitio web dentro de un iframe. Puedes hacerlo enviando la cabecera HTTP X-Frame-Options. El encabezado proporciona al propietario del sitio web control sobre el uso de iframes u objetos, de modo que la inclusión de una página web dentro de un marco/frame puede prohibirse con la directiva deny: **X-Frame-Options: deny**	
2. Vulnerabilidad	**Apache HTTP Server Buffer Overflow Vulnerability:** Apache HTTP Server, coloquialmente llamado Apache, es un software de servidor web multiplataforma gratuito y de código abierto. En las versiones afectadas de Apache HTTP Server, un envío de solicitud cuidadosamente elaborado puede provocar un desbordamiento de búfer ocasionando una denegación de servicio.
Recomendaciones	
Update Apache	Se recomienda a los clientes que actualicen a Apache HTTP Server (versión actualizada 2.4.57) a una versión posterior para remediar esta vulnerabilidad.
Instalar, actualizar Apache Server	

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el MEC. Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS

Grupo Horus S.A.

G. SITE-WEB

https://XXX - ANONIMIZADO.gov.py/

1. Vulnerabilidad	**Cross-Site Scripting:** la aplicación web refleja caracteres potencialmente peligrosos, como comillas simples, comillas dobles y corchetes angulares. Estos caracteres se usan comúnmente para ataques de inyección de HTML, como secuencias de comandos entre sitios (XSS).
Recomendaciones	
Content Security Policy	Los contenidos activos en páginas web, como por ejemplo JavaScript, CSS o ActiveX, plantean riesgos de seguridad para los usuarios de Internet y los gestores de páginas web y pueden manipularse. Para que las páginas de Internet puedan utilizarse sin preocupaciones, existe lo que se conoce como Content Security Policy (CSP), cuyo papel consiste en proteger a las páginas frente a ataques perjudiciales y es compatible con la mayoría de navegadores web.
Ejemplos de CSP: 1. script-src "https://example.com:443" – Solo se permiten scripts de este dominio por HTTPS. 2. script-src 'none' – No se pueden cargar scripts. 3. script-src 'self' – Solo pueden cargarse scripts que tengan el mismo origen que la página actual, pero no el de los subdominios. 4. script-src https: – Se pueden cargar scripts de cualquier dominio siempre que empiecen por HTTPS. 5. script-src example.com – Se pueden cargar scripts de este dominio. 6. script-src *.example.com – Se permiten scripts de este y de todos los dominios. 7. img-src data: – Pueden cargarse imágenes por medio de enlaces de datos.	
2. Vulnerabilidad	**Apache HTTP Server Buffer Overflow Vulnerability**: Apache HTTP Server, coloquialmente llamado Apache, es un software de servidor web multiplataforma gratuito y de código abierto. En las versiones afectadas de Apache HTTP Server, un envío de solicitud cuidadosamente elaborado puede provocar un desbordamiento de búfer ocasionando una denegación de servicio.
Recomendaciones	
Update Apache	Se recomienda a los clientes que actualicen a Apache HTTP Server (versión actualizada 2.4.57) a una versión posterior para remediar esta vulnerabilidad.
Instalar, actualizar Apache Server	

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el MEC. Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS

GRUPO HORUS S.A.

H. SITE-WEB

https://XXX - ANONIMIZADOescolar.mec.gov.py/

1. Vulnerabilidad	**Use of JavaScript Library with Known Vulnerability:** La aplicación web utiliza una biblioteca de JavaScript que se sabe que contiene al menos una vulnerabilidad.
Recomendaciones	
Update Librerías	Se recomienda la actualización de las dependencias y librerías instaladas.

Debe existir un proceso de administración de parches para:

- Eliminar las dependencias no utilizadas, las funciones, los componentes, los archivos y la documentación innecesarios.
- Haga un inventario continuo de las versiones de los componentes del lado del cliente y del lado del servidor (por ejemplo, marcos, bibliotecas) y sus dependencias utilizando herramientas como versiones, OWASP Dependency Check, retire.js, etc. Monitoree continuamente fuentes como Common Vulnerability and Exposures (CVE) y National Vulnerability Database (NVD) para detectar vulnerabilidades en los componentes.
- Solo obtenga componentes de fuentes oficiales a través de enlaces seguros. Prefiera los paquetes firmados para reducir la posibilidad de incluir un componente malicioso modificado.
- Supervise las bibliotecas y los componentes que no reciben mantenimiento o que no crean parches de seguridad para versiones anteriores. Si no es posible aplicar parches, considere implementar un parche virtual para monitorear, detectar o proteger contra el problema descubierto.
- Cada organización debe garantizar un plan continuo para monitorear, clasificar y aplicar actualizaciones o cambios de configuración durante la vida útil de la aplicación o cartera.

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el MEC. Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS

GRUPO HORUS S.A.

I. SITE-WEB

https://XXX - ANONIMIZADO.mec.gov.py/

1. Vulnerabilidad	**Clickjacking**: es un ataque basado en la interfaz que engaña a los usuarios de un sitio web para que sin saberlo hagan clic en enlaces maliciosos. En clickjacking, los atacantes incrustan sus enlaces maliciosos en botones o páginas legítimas en un sitio web
Recomendaciones	
X-FRAME-OPTIONS	El encabezado X-Frame-Option permite tres valores. ● DENY, que prohíbe mostrar la página dentro de un marco ● SAMEORIGIN, que permite mostrar la página dentro de un marco, siempre que permanezca en el mismo dominio ● PERMITIR-DESDE URI, que permite la visualización de la página dentro de un marco, pero solo en un URI específico (Identificador uniforme de recursos), por ejemplo, solo dentro de una página web específica en particular.
Para prevenir los ataques de clickjacking es pedir al navegador que bloquee cualquier intento de cargar tu sitio web dentro de un iframe. Puedes hacerlo enviando la cabecera HTTP X-Frame-Options. El encabezado proporciona al propietario del sitio web control sobre el uso de iframes u objetos, de modo que la inclusión de una página web dentro de un marco/frame puede prohibirse con la directiva deny: **X-Frame-Options: deny**	

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el MEC. Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS

GRUPO HORUS S.A.

J. SITE-WEB

https://XXX - ANONIMIZADO.mec.edu.py/

1. Vulnerabilidad	**Vulnerabilidad basada en rutas:** se descubrió un archivo, directorio o lista de directorios potencialmente confidencial en el servidor web.
Recomendaciones	
Path Disclosure	Las vulnerabilidades de divulgación de ruta completa (FPD) permiten al atacante ver la ruta al archivo/raíz web. por ejemplo: /inicio/omg/htdocs/archivo/. Ciertas vulnerabilidades, como el uso de la consulta load_file() (dentro de una inyección SQL) para ver el código fuente de la página, requieren que el atacante tenga la ruta completa al archivo que desea ver.

La forma de proteger su servidor web de los ataques de divulgación de ruta completa es editando el archivo php.ini de su servidor para:
 	
Deshabilitar el informe de errores:
error_reporting(0);
Ocultar mensajes de error:
display_errors(0);	

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el MEC. Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS

GRUPO HORUS S.A.

K. SITE-WEB

https://mec.gov.py/XXX - Anonimizado/

1. Vulnerabilidad	**Vulnerabilidad basada en rutas:** se descubrió un archivo, directorio o lista de directorios potencialmente confidencial en el servidor web.
Recomendaciones	
Path Disclosure	Las vulnerabilidades de divulgación de ruta completa (FPD) permiten al atacante ver la ruta al archivo/raíz web. por ejemplo: /inicio/omg/htdocs/archivo/. Ciertas vulnerabilidades, como el uso de la consulta load_file() (dentro de una inyección SQL) para ver el código fuente de la página, requieren que el atacante tenga la ruta completa al archivo que desea ver.

La forma de proteger su servidor web de los ataques de divulgación de ruta completa es editando el archivo php.ini de su servidor para:
 	
Deshabilitar el informe de errores:
error_reporting(0);
Ocultar mensajes de error:
display_errors(0);	

1. Vulnerabilidad	**WordPress XML-RPC Pingback Vulnerability:** XML-RPC es una característica de WordPress que permite que los datos se transmitan, con HTTP actuando como el mecanismo de transporte y XML como el mecanismo de codificación. Dado que WordPress no es un sistema encerrado en sí mismo y ocasionalmente necesita comunicarse con otros sistemas, la intención era realizar ese trabajo. Por ejemplo, supongamos que quisieras publicar en tu sitio desde tu dispositivo móvil ya que tu computadora no está cerca. Podrías usar la función de acceso remoto habilitada por xmlrpc.php para hacerlo. Las funciones principales de xmlrpc.php eran permitirte conectarte a tu sitio a través de un teléfono móvil, implementar trackbacks y pingbacks desde otros sitios, y algunas funciones asociadas con el plugin Jetpack.
Recomendaciones	
WordPress XML-RPC	Hay cuatro formas en que un atacante podría abusar de la API XML-RPC de WP (específicamente, el método): pingback.ping • **Recopilación de Intel** : el atacante puede buscar puertos específicos en la red interna del objetivo • **Escaneo de puertos** : el atacante puede escanear puertos de hosts en la red interna • **Ataques DoS** : el atacante puede hacer pingback a través de una gran cantidad de sitios para un ataque DoS • **Hackeo de enrutadores** : el atacante puede reconfigurar un enrutador interno en la red
Si no está utilizando la funcionalidad XML-RPC, puede bloquear la funcionalidad agregando un la configuración en el .htaccess :	

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el MEC. Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS

GRUPO HORUS S.A.

```
# protect xmlrpc
<IfModule mod_alias.c>
        RedirectMatch 403 /xmlrpc.php
</IfModule>
```

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el MEC. Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS

GRUPO HORUS S.A.

6. Recomendaciones para Sitios Internos

Cuando se trata de garantizar la seguridad de aplicaciones internas, es importante adoptar un enfoque sólido para proteger los activos y datos de tu organización.

Aquí tienes algunas recomendaciones de seguridad para aplicaciones internas:

Autenticación y Autorización: Implementa un sólido sistema de autenticación para garantizar que solo los usuarios autorizados puedan acceder a la aplicación. Además, establece un sistema de autorización que limite el acceso de los usuarios a las funciones y datos necesarios para realizar sus tareas.

Actualización y Parcheo: Mantén todas las aplicaciones y componentes de software actualizados con los últimos parches de seguridad. Esto ayuda a prevenir la explotación de vulnerabilidades conocidas.

Cifrado de Datos: Utiliza cifrado para proteger los datos tanto en reposo como en tránsito. Esto garantiza que los datos confidenciales estén protegidos en caso de pérdida o robo de dispositivos, o durante la transmisión.

Gestión de Contraseñas: Implementa políticas de gestión de contraseñas sólidas, que incluyan requisitos de complejidad, caducidad de contraseñas y autenticación de dos factores (2FA) cuando sea posible.

Control de Acceso Basado en Roles: Asigna roles y permisos de usuario de manera adecuada. Los usuarios deben tener acceso solo a las áreas y funciones que son relevantes para su trabajo.

Pruebas de Penetración: Realiza pruebas de penetración regulares para identificar posibles vulnerabilidades en la aplicación. Esto incluye pruebas de seguridad internas y externas.

Monitoreo y Registro: Implementa un sistema de monitoreo para rastrear actividades inusuales o potencialmente maliciosas. Lleva registros (logs) detallados de las acciones de los usuarios y eventos del sistema para una auditoría y detección de incidentes.

Seguridad en el Desarrollo: Integra la seguridad desde el inicio del ciclo de desarrollo de la aplicación. Utiliza buenas prácticas de seguridad, como la validación de entrada, la prevención de inyección de SQL y la desinfección de datos.

Gestión de Sesiones: Asegúrate de que las sesiones de usuario estén protegidas y bien gestionadas. Utiliza tokens de sesión seguros y configura tiempos de expiración adecuados.

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el MEC. Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS

GRUPO HORUS S.R.

Actualizaciones de Seguridad: Mantén actualizados los componentes y bibliotecas de terceros utilizados en la aplicación. Las vulnerabilidades en bibliotecas externas pueden ser una amenaza significativa.

Concienciación de los Usuarios: Proporciona capacitación en seguridad a los usuarios para ayudarles a reconocer posibles amenazas, como correos electrónicos de phishing, y promover buenas prácticas de seguridad.

Segregación de Redes: Si es posible, separa la red de las aplicaciones internas de otras redes para limitar el acceso no autorizado.

Recuperación de Desastres: Implementa planes de recuperación de desastres para garantizar la disponibilidad de la aplicación en caso de interrupciones o incidentes de seguridad.

Estas recomendaciones de seguridad son fundamentales para proteger las aplicaciones internas de tu organización. Es importante mantener una mentalidad proactiva en cuanto a la seguridad y estar al tanto de las últimas amenazas y mejores prácticas de seguridad.

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el MEC. Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS
GRUPO HORUS S.A.

1. Default Tomcat User and Password (apache-tomcat-default-password)

Affected Nodes: 1	Additional Information: Existencia de Exploit	Status ACTIVO

Cambie la contraseña de la cuenta del administrador del servicio de Tomcat.

El servicio Tomcat tiene una cuenta de administrador establecida en una configuración predeterminada. Esto se puede cambiar en conf/tomcat-users.xml

Esto solucionará el siguiente problema: usuario y contraseña predeterminados de Tomcat (apache-tomcat-default-password).

2. Postgres default account: postgres/no password

Affected Nodes: 7	Additional Information: Existencia de Exploit	Status ACTIVO

Establezca una contraseña para la cuenta 'postgres'. Esto generalmente se hace editando el archivo 'pg_hba.conf'

Esto solucionará el siguiente problema: Cuenta predeterminada de Postgres: postgres/sin contraseña (postgres-default-account-postgres-nopassword).

Restringir el acceso a la base de datos

Configure el servidor de la base de datos para que solo permita el acceso a sistemas de confianza. Por ejemplo, el estándar PCI DSS requiere que coloque la base de datos en una zona de red interna, separada de la DMZ

Esto solucionará el siguiente problema: Acceso abierto a la base de datos (acceso abierto a la base de datos).

3. Samba RPC unauthenticated remote code execution (CVE-2012-1182)

Affected Nodes: 2	Additional Information: Existencia de Exploit	Status ACTIVO

Estas vulnerabilidades se pueden resolver realizando los siguientes 3 pasos.

1. Actualizar a la última versión de Samba
2. Alternativamente, los parches pueden estar disponibles en http://www.samba.org/samba/history/security.html.
3. Se recomienda que utilice el administrador de paquetes de su sistema operativo para actualizar si es posible.

Adicionalmente configurar la firma SMB para Samba

Configure Samba para habilitar o requerir la firma SMB según corresponda. Para habilitar la firma SMB, coloque lo siguiente en Samba

archivo de configuración, la configuración default se encuentra en smb.conf, en la sección global:

firma del servidor = auto

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el MEC. Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS

GRUPO HORUS S.A.

Para solicitar la firma SMB, cambiel:

firma del servidor = obligatorio

4. PHP Vulnerability: CVE-2015-0235

Affected Nodes: 50	Additional Information: Existencia de Exploit	Status ACTIVO

Estas vulnerabilidades se pueden resolver realizando los siguientes pasos.

Actualice a la última versión de PHP

Descargue y aplique la actualización desde: http://www.php.net/downloads.php
La última versión de PHP es 8.2.3
Esto indirectamente resolverá 1,136 problemas:

5. Apache Tomcat: Important: Remote Code Execution on Windows (CVE-2019-0232)

Affected Nodes: 12	Additional Information: Existencia de Exploit	Status ACTIVO

Actualice a la última versión de Apache Tomcat

Descargue y aplique la actualización desde: http://archive.apache.org/dist/tomcat/tomcat-10/v10.1.9/

La última versión de Apache Tomcat es 10.1

Esto indirectamente resolverá 71 problemas:

6. Webmin: Unauthenticated Remote Code Execution

Affected Nodes: 21	Additional Information: Existencia de Exploit	Status ACTIVO

Actualizar a la última versión de Webmin

Descargue y aplique la actualización desde: https://sourceforge.net/projects/webadmin/files/webmin/

Actualice a la última versión de Webmin.
Esto solucionará el siguiente problema: CVE-2019-15107: Webmin: Ejecución de código remoto no autenticado (http-webmin-cve-2019-15107).

7. PostgreSQL class A vulnerability in core server: CVE-2013-1899

Affected Nodes: 21	Additional Information: Existencia de Exploit	Status ACTIVO

Estas vulnerabilidades se pueden resolver con un solo paso.

Actualice a la última versión de PostgreSQL

Descargue y aplique la actualización desde: http://www.postgresql.org/download/

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el MEC. Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS

GRUPO HORUS S.A.

8. HTTP TRACE Method Enabled

Affected Nodes: 104	Additional Information: Existencia de Exploit	Status ACTIVO

Deshabilitar el método HTTP TRACE para Apache
Apache HTTPD, Apache Tomcat
Las versiones más recientes de Apache (1.3.34 y 2.0.55 y posteriores) proporcionan una directiva de configuración llamada TraceEnable. Para denegar solicitudes, agregue la siguiente línea a la configuración del servidor:

TraceEnable off

Para versiones anteriores del servidor web Apache, use el módulo mod_rewrite para denegar las solicitudes TRACE:

RewriteEngine On
RewriteCond %{REQUEST_METHOD} ^TRACE
RewriteRule .* - [F]

En Apache Tomcat, HTTP Trace se puede deshabilitar agregando restricciones de seguridad en la especificación de Java Servlet dentro del archivo de configuración web.xml y estableciendo el atributo allowTrace="False" en el conector HTTP en server.xml.

9. Apache Tomcat: Important: Remote Code Execution (CVE-2017-12617)

Affected Nodes: 104	Additional Information: Existencia de Exploit	Status ACTIVO

Actualice a la última versión de Apache Tomcat

Descargue y aplique la actualización desde: http://archive.apache.org/dist/tomcat/tomcat-10/v10.1.9/

La última versión de Apache Tomcat es 10.1.9

10. Default SSH password: admin password "admin"

Affected Nodes: 5	Additional Information: Existencia de Exploit	Status ACTIVO

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el MEC. Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS
GRUPO HORUS S.A.