CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Aumento de ciberataques

Fecha: 08/08/2022

Problemática: Ciberataques de tipo DEFACEMENT

Correlativo: AA-0011

Institución / Sector: Instituciones Públicas y Privadas

CONTEXTO

Se alerta sobre el aumento de ciberataques de tipo DEFACEMENT que están afectando a sitios web de gobiernos municipales, que de forma inusual tienen como patrón la desfiguración de sitios web.

SITUACIÓN

De acuerdo a la investigación perpetrada por el Centro Estratégico de Monitoreo, este tipo de ataques generalmente tienen como objetivo la desconfiguración de sitios web.

Puntos clave:

Caso 1: Los ciberdelincuentes aprovechándose de la vulnerabilidad identificada en el gestor de contenidos de Wordpress, realizaron la inserción del fichero vz.txt (munichinautla. gob.gt/vz.txt) con su alias; el cual inyectaba scripts redirectores hacia una web de comercio electrónico (jtokrise.com).

Caso 2: Los ciberdelincuentes aprovechándose de la vulnerabilidad identificada en el gestor de contenidos de Wordpress, realizaron la inserción del fichero 1.php (scp.gob.gt/1.php) con su alias; el cual infectada con SEO Spam mostrando contenido explícito.

Nivel de priorización

Prioridad Urgente / No Urgente	Actualización Seguimiento/Preventiva/Resiliente
Urgente	Resiliente

Matriz de Evaluación

Riesgo Alto/ Medio/ Bajo	Nivel de Afectación		
	Integridad	Disponibilidad	Confidencialidad
	Alta	Alta	Alta

RECOMENDACIONES

Ante esta alerta se insta a las instituciones de gobierno municipal, atender las siguientes recomendaciones mínimas para proteger su sitio web:

1. Cambie el nombre de usuario de administrador de acceso a Wordpress
2. Utilice contraseñas fuertes y seguras
3. Mantenga actualizado tanto la versión de Wordpress como los plugins que utiliza
4. Proteja el archivo de configuración de Wordpress wp-config.php
5. Limite los intentos de acceso

DICCIONARIO DE DATOS

1. Ciberdelincuente: Persona que se aprovecha de fallas de seguridad encontradas en plataformas, programas o sistemas a título personal
2. Wordpresss: Sistema de administración de contenidos web.
3. Sitio web: Colecciones de páginas web relacionadas y comunes a un dominio a internet.
4. Fichero: Secuencia de bytes almacenados en un dispositivo.
5. Script: Archivos o secciones de código escrito en lenguajes de programación.
6. Comercio electrónico: Consiste en la compra y venta de productos o de servicios a través de internet.
7. SEO: Conjunto de acciones orientadas a mejorar el posicionamiento de un sitio web
8. Spam: Correo electrónico no solicitado, normalmente conteniendo publicidad.

REFERENCIAS

1. http://www.zone-h.org/archive/notifier=aDriv4?hz=1
2. http://www.zone-h.org/mirror/id/39770633
3. https://kinsta.com/es/blog/seguridad-wordpress/
4. https://wordpress.com/es/go/

ÁREA PARA DEFINICIONES