ALERTA DE SEGURIDAD

CSIRT-RD

Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

FECHA DE PUBLICACIÓN: 7 DE FEBRERO 2022

PRESIDENCIA DE LA REPÚBLICA DOMINICANA

MINISTERIO DE LA PRESIDENCIA

CNCS CENTRO NACIONAL DE CIBERSEGURIDAD REPÚBLICA DOMINICANA

CSIRT-RD

Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

ALERTA DE SEGURIDAD

- **ID** INC-01424-R5C2
- **TLP** Blanco
- **Tipo de incidente** Defacement
- **Categoría** Intrusión

DETALLES DE ALERTA

El Equipo Nacional de Respuesta a Incidentes CSIRT-RD, comparte los indicadores de compromisos asociados a ataques contra servicios de portales web de República Dominicana que se han visto recientemente involucradas en ataques relacionados con alteraciones de páginas web en el país.

INDICADORES DE COMPROMISO (IoC)

IP:

- 185[.]220[.]101[.]86
- 193[.]218[.]118[.]158
- 185[.]220[.]101[.]8
- 185[.]220[.]101[.]184
- 5[.]199[.]143[.]202
- 185[.]220[.]101[.]17
- 185[.]220[.]101[.]41
- 79[.]136[.]1[.]46
- 23[.]128[.]248[.]28
- 5[.]2[.]69[.]50
- 185[.]67[.]82[.]114
- 185[.]220[.]102[.]241
- 185[.]220[.]101[.]73
- 104[.]244[.]76[.]127
- 89[.]58[.]27[.]84

El defacement o desconfiguración de un sitio web es un ataque que cambia la apariencia visual del sitio o una página web. Este tipo de ataques pueden tener diferentes motivaciones y comúnmente se realizan aprovechando una vulnerabilidad presente en el sitio web.

RECOMENDACIONES

1. Se recomienda mantener actualizados los componentes y software utilizado en los servidores web.
2. Mantener un monitoreo continuo sobre el portal web y conservar implementada buenas prácticas de seguridad sobre el mismo.
3. Implementar un proceso de respaldo para el portal web, como medida preventiva de recuperación.
4. Se recomienda implementar una política de contraseñas, utilizando credenciales robustas en los servicios web.
5. Se recomienda limitar el acceso a los paneles de administración de los manejadores de contenidos como WordPress y Joomla para evitar ataques de fuerza bruta, pudiendo limitar el acceso desde direcciones IP conocidas o aplicar controles que impidan realizar este tipo de ataques, como es la implementación de autenticación de dos factores (2FA).