Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

Actualización

Extracción de Información de Desarrollo Relacionado al Gobierno de República Dominicana

25/Noviembre/2022

Contenido

INTRODUCCIÓN – ACTUALIZACIÓN

El día 18 de noviembre de 2022, Se envío un boletín con información relevante sobre una brecha de extracción de información relacionado a algunas instituciones de gobierno de Republica Dominicana, dentro del mismo se identifico un error en la información suministrada.

Se aclara en el siguiente boletín, lo siguiente:

- Nuestro monitoreo en foros de Deep Web incluye la búsqueda activa de indicadores de compromiso de todos los países de Centroamérica y Caribe, siendo esto, todo lo relacionado con el TLD ".do".

- Dentro de nuestro monitoreo, se identifico dentro del siguiente enlace la extracción de información de un sitio web, siendo la fuente de información la siguiente: https://breached.vc/Thread-Source-Code-Dominican-Republic-Services-Web-server-Source-Code-Leak

- Al descargar la información suministrada en el foro en formato ZIP, se identifica que dicha información es más una extracción de información de un sitio de desarrollo dentro de una institución de gobierno mediante algún CRAWLER más que el código fuente de alguna institución mencionada anteriormente en el boletín.

- Identificando la brecha de seguridad, validamos que la vulnerabilidad del servicio en el servidor expuesto es una mala configuración que se tiene dentro del servicio web por medio del uso de la funcionalidad de INDEXES que permite el servicio de APACHE, esta información se detalla a continuación: https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/directory-listing-apache/

- Ninguna de las instituciones mencionadas anteriormente por el boletín estuvo afectada directamente a esta vulnerabilidad, únicamente se encontraba su imagen de logo dentro de la información extraída del archivo comprimido ZIP.

- El impacto de la filtracion tambien fue cambiado de alto a medio, ya que esta amenza no significa un riesgo alto.

- Por último, las recomendaciones listadas en el boletín inicial fueron cambiadas ya que no estaban alineadas con el tipo de amenaza antes mencionada.

A continuación, se adjunta la información recolectada.

FILTRACIÓN DE INFORMACION.

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2022_11_18_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Medio
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	11/18/2022 ACTUALIZACION 11/23/2022
Es día cero (0 day):	No

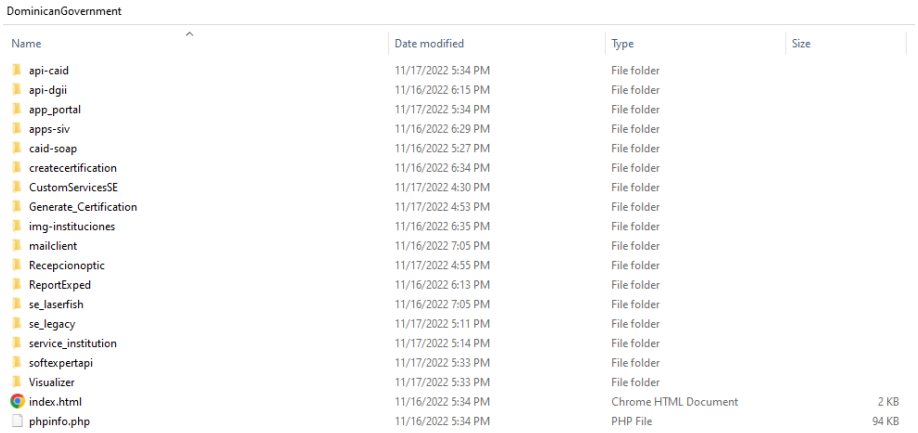
RESUMEN

EL usuario **Sc0rp10n** mediante la publicación de https://breached.vc/Thread-Source-Code-Dominican-Republic-Services-Web-server-Source-Code-Leak ha hecho público un archivo comprimido ZIP con la información extraída de un servidor dentro del dominio "gob.do" en donde se puede identificar información de uso restringido en el ambiente de desarrollo de la institución.

A continuación, se identifican imágenes de la información descargada por el comprimido ZIP.

Filename: DominicanGovernment.zip

SHA256: C8692CC9791AD813C88E3C2B45A335AAF2E4ACD16F57EADD4B49244F7590FF7A



DominicanGovernment

Name	Date modified	Type	Size
api-caid	11/17/2022 5:34 PM	File folder	
api-dgii	11/16/2022 6:15 PM	File folder	
app_portal	11/17/2022 5:34 PM	File folder	
apps-siv	11/16/2022 6:29 PM	File folder	
caid-soap	11/16/2022 5:27 PM	File folder	
createcertification	11/16/2022 6:34 PM	File folder	
CustomServicesSE	11/17/2022 4:30 PM	File folder	
Generate_Certification	11/17/2022 4:53 PM	File folder	
img-instituciones	11/16/2022 6:35 PM	File folder	
mailclient	11/16/2022 7:05 PM	File folder	
Recepcionoptic	11/17/2022 4:55 PM	File folder	
ReportExped	11/16/2022 6:13 PM	File folder	
se_laserfish	11/16/2022 7:05 PM	File folder	
se_legacy	11/17/2022 5:11 PM	File folder	
service_institution	11/17/2022 5:14 PM	File folder	
softexpertapi	11/17/2022 5:33 PM	File folder	
Visualizer	11/17/2022 5:33 PM	File folder	
index.html	11/16/2022 5:34 PM	Chrome HTML Document	2 KB
phpinfo.php	11/16/2022 5:34 PM	PHP File	94 KB

Inventario de archivos dentro del repositorio

```
<strong>Error con la conexion</strong> <br />Array
(
    [Database] => Sesuitedb
    [UID] => consultauser
    [PWD] => Admin@1234
)
1
```

Información sensible dentro de algunos archivos

Imágenes dentro de una carpeta (La institución afectada no se encuentra en este listado)

Se identifico que la vulnerabilidad dentro del servidor de desarrollo se encuentra activa a la fecha de esta publicación.

RECOMENDACIONES

- Se recomienda realizar un bastionado de seguridad a cualquier servicio que se encuentre publicado hacia Internet, siendo esto ambientes de producción como desarrollo.

- Se recomienda realizar una auditoria de sistemas en busca de vulnerabilidades expuestas a internet.

- Se recomienda soluciones de cortafuegos de aplicación (Capa 7) para la protección de todos los servicios públicamente expuestos por Internet (HTTPS).

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

Sitio Web: https://www.devel.group/reporta-un-incidente