Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

F código fuente de servidores web relacionados al gobierno de Republica Dominicana.

18/Noviembre/2022

Contenido

Introducción

El día 17 de noviembre mediante breached.vc un usuario realizo un post afirmando poseer código fuente y otros datos de gran valor extraídos de uno de los servidores web del gobierno de Republica Dominicana.

Filtración de Web Servers de Republica Dominicana.

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:	Alto
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	11/18/2022
Es día cero (0 day):	No

Resumen

EL usuario Sc0rp10n mediante breached,vc ha hecho público un listado especificando el tipo de información filtrada desde servidores pertenecientes al gobierno dominicano.

La información filtrada se compone de los siguientes activos:

- Archivos de control Git.

- Archivos .env.

- Contraseñas SMTP.

- Contraseñas de la base de datos.

- Contraseñas del panel de administración.

- Código fuente de la API de producción.

Hasta el momento ninguna entidad gubernamental de Republica Dominicana ha emitido un comunicado que pueda confirmar esta filtración.

Dentro de la filtración se encuentran todos los ficheros anunciados por el actor malicioso, pero no se observa ninguna nota de rescate o algún fichero malicioso que permita identificar si la vulneración al equipo desde el que se filtro toda la información fue generada por una campaña de ransomware o algún otro método de extracción remota.

DominicanGovernment/apps-siv/counter/.git/objects/19/index.html	.html
DominicanGovernment/apps-siv/counter/.git/objects/1a/index.html	.html
DominicanGovernment/apps-siv/counter/.git/objects/1b/index.html	.html
DominicanGovernment/apps-siv/counter/.git/objects/1c/index.html	.html
DominicanGovernment/apps-siv/counter/.git/objects/1d/index.html	.html
DominicanGovernment/apps-siv/counter/.git/objects/1e/index.html	.html
DominicanGovernment/apps-siv/counter/.git/objects/1f/index.html	.html
DominicanGovernment/apps-siv/counter/.git/objects/20/index.html	.html
DominicanGovernment/apps-siv/counter/.git/objects/21/index.html	.html
DominicanGovernment/apps-siv/counter/.git/objects/22/index.html	.html
DominicanGovernment/apps-siv/counter/.git/objects/23/index.html	.html
DominicanGovernment/apps-siv/counter/.git/objects/24/index.html	.html
DominicanGovernment/apps-siv/counter/.git/objects/26/index.html	.html

Las instituciones afectadas por esta Filtración son:

- Centro de atención integral para la discapacidad.
- CAASD
- Ministerio de Turismo
- Ayuntamiento Santo Domingo Este
- Departamento Aeroportuario
- Edesur
- Instituto Nacional de la Vivienda
- Dirección general de impuestos internos.
- INABIMA

De momento no se tiene mas conocimiento sobre nuevas filtraciones o ataques a instituciones gubernamentales/privadas de este País.

Recomendaciones

- Aplicar buenas prácticas en sus servidores como ser: Hardening, DMZ, Control de usuarios con acceso administrativo e historial de inicios de sesión y configuraciones realizadas por usuarios dentro de los equipos.

- Como medida de prevención, agregue los indicadores de compromiso que Devel ha recolectado sobre ransomware y botnets. Puede visualizarlos en este enlace.

- Solicite a su SOC monitoreo permanente sobre actividad sospechosa en sus servidores, con el fin de poder reaccionar ante cualquier intento de infiltración no deseado.

Noticia Completa

https://devel.group/blog/filtran-codigo-fuente-desde-servidores-web-de-republica-dominicana/

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

WhatsApp: +(502) 5124 9536

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