ALERTA DE SEGURIDAD

CSIRT-RD

Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

FECHA DE PUBLICACIÓN: 22 DE ENERO 2021

© Todos los derechos reservados

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

El presente documento es propiedad del **Centro Nacional de Ciberseguridad (CNCS),** y fue generado mediante el análisis de varias fuentes de terceras partes y una investigación del equipo CSIRT-RD.

ALERTA DE SEGURIDAD

- **TLP** Blanco
- **Tipo de incidente** Explotación de Vulnerabilidades
- **Categoría** Intrusión
- **Nivel de peligrosidad CRITICO**

DETALLES DE ALERTA

El Equipo Nacional de Respuesta a Incidentes CSIRT-RD ha identificado varios indicadores de compromiso de ataque que se encuentran realizando explotación de vulnerabilidades en el ciberespacio nacional, con el objetivo de afectar la disponibilidad de los servicios tecnológicos de la institución y el secuestro de la información para solicitar pago de rescate por la misma. Los mismos se encuentran utilizando diferentes vectores de entrada tales como correos de suplantación, vulnerabilidad en los sistemas de protección y acceso remoto vía SSL VPN a través de equipos comprometidos de usuarios en teletrabajo.

INDICADORES DE COMPROMISO (IoC)

VULNERABILIDADES

El CSIRT-RD ha observado la actividad maliciosa desde las direcciones IP pertenecientes al bloque 45.155.205.0/24 realizando exploraciones para realizar la ejecución de código remoto PHP mediante los datos HTTP POST explotando la vulnerabilidad CVE-2017-9841, CVE-2019-9082 y para servicios web JSON CVE-2020-7961.

Hallazgos importantes;

- Intento de recuperación de información del sistema de instancias de APACHE SOLR, incluida la información del nodo que podría utilizarse para fines maliciosos. (CVE-2019-17558)

- Escaneos para realizar conexiones TLS/SSL.

- Escaneo en busca de Docker DAEMOS y bases de datos MySQL expuestos.

- Aprovechamiento de conexiones de red privada (VPN) Cisco AnyConnect SSL para habilitar inicios de sesión remotos en la red victima, posiblemente utilizando una vulnerabilidad del protocolo SMTP. (CVE-2019-10149)

- Enumeración y explotación de vulnerabilidades en SSL VPN de Fortinet para el acceso inicial. (CVE-2018-13379)

- Enumeración y explotación de una vulnerabilidad de Windows netlogon para obtener acceso a los servidores de Active Directory para escalar privilegios, así como comprometer dispositivos de red y mantener la persistencia. (CVE-2020-1472)

RECOMENDACIONES

1. Realizar el análisis correspondiente para el bloqueo a los indicadores de compromiso expuestos por un mínimo de 30 días, indicados en este documento.
2. Recomendamos tener precaución al momento de acceder a enlaces suministrados mediante medios de mensajería.
3. Mantener actualizadas las plataformas y sistemas de información según las recomendaciones del proveedor y en especial priorizar las actualizaciones para aplicaciones externas y servicios de acceso remoto.
4. Realizar contacto inmediato con el Equipo Nacional de Respuesta a Incidentes Ciberneticos (CSIRT-RD), a través del correo incidentes@csirt.gob.do, para reportar cualquier acción sospechosa o posible incidente de ciberseguridad antes de realizar una acción.
5. Realizar campañas de concientización periódica a todos los usuarios de la institución.