PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno y Transformación Digital

Siempre con el pueblo

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Centro Nacional de Seguridad Digital

asbanc
ASOCIACIÓN DE BANCOS DEL PERÚ

Lima, 12 de mayo de 2022

N° 128-2022-CNSD

La presente **Alerta Integrada de Seguridad Digital** corresponde a un análisis técnico periódico realizado por el Comando Conjunto de las Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aérea del Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en el marco de la Seguridad Digital del Estado Peruano.

El objetivo de esta alerta **es informar a los responsables de la seguridad digital de las entidades públicas y las empresas privadas sobre las amenazas en el entorno digital** para advertir las situaciones que pudieran afectar la continuidad de sus servicios en favor de la población.

Las marcas y logotipos de empresas privadas y/o entidades públicas se reflejan para ilustrar la información que los ciudadanos reciben por redes sociales u otros medios y que atentan contra la confianza digital de las personas y de las mismas empresas **de acuerdo con lo establecido por el Decreto de Urgencia 007-2020**.

La presente Alerta Integrada de Seguridad Digital es información netamente especializada para informar a las áreas técnicas de entidades y empresas.

Contenido

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 128	Fecha: 12-05-2022
		Página 4 de 8

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Ransomware Conti presume atacar servicios críticos de Perú		
Tipo de ataque	Ransomware	Abreviatura	Ransomware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de subfamilia	C01
Clasificación temática familia	Código Malicioso		

Descripción

I. DATOS GENERALES:

El grupo ruso que se especializa en vulnerar plataformas públicas, secuestrando datos y sistemas, obligó a declarar el Estado de Emergencia en Costa Rica. Expertos advierten que este puede ser sólo uno de muchos otros ataques a entidades oficiales de países como Perú, Chile y México, entre otros.

II. EVIDENCIA:

- Conti, con sede en Rusia, fue detectado por primera vez en 2019 y fue uno de los grupos cibercriminales más activos en 2021. En noviembre de ese año, el número de víctimas acumuladas desde sus inicios daba cuenta que es el grupo que más organizaciones afectó con 600.

- *"Todos los documentos descargados se clasifican como secretos. Trabajamos exclusivamente por dinero, no perseguimos otros objetivos",* presume el grupo de ciberdelincuentes en sus canales de difusión, y reportan expertos de ciberseguridad.

- Steph Shample, experto en seguridad cibernética y miembro del Middle East Institute, explicó a fuentes abiertas, que Conti está extremadamente bien organizado y es cuidadoso al seleccionar objetivos de los cuales roba grandes cantidades de datos confidenciales.

III. TEMA:

- Se presume que los ciberdelincuentes usan malware como Trickbot y Emotet para el acceso inicial a una organización. La defensa contra tales ataques se complica por errores humanos. Cuando un solo empleado hace clic en un enlace malicioso, toda la infraestructura crítica de una organización puede verse comprometida.

  "Obtendrán credenciales adicionales. Pueden leer correos electrónicos privados y leer chats privados en cualquier empresa. Solo se necesita vulnerabilidad y luego todo está disponible", señala Shample.

- En medio de ataques de ransomware a gran escala en Costa Rica y Perú, supuestamente ambos ejecutados por la infame banda de ransomware Conti, el Departamento de Estado de EEUU emitió un comunicado el 6 de mayo ofreciendo una recompensa de hasta US$ 10 millones por información que conduzca a la identificación o ubicación de personas involucradas.

- La banda de ciberdelincuentes presume desde la Deep web ser una amenaza para los servicios críticos de Perú, incluido el servicio de agua y de electricidad.

IV. CONCLUSIÓN:

- De acuerdo al portavoz del Departamento de Estado, Ned Price, el FBI estima que más de 1.000 víctimas del grupo Conti han pagado un total de más de US$ 150 millones en pagos de ransomware.

- En los primeros cuatro meses del 2022, Check Point Research (CPR), informó que, en promedio, una de cada 60 organizaciones en todo el mundo se ha visto afectada por un intento de ataque de ransomware cada semana, un aumento interanual del 14%.

V. RECOMENDACIÓN:

- Concientizar al equipo de trabajo en todos los niveles de la institución.
- Contar con directrices de respaldo y protección de datos.
- Contar con directrices vigentes de autenticación multifactor en los sistemas de información.
- Contar con soluciones de ciberseguridad vigentes y actualizadas.
- Contar con un plan de respuesta ante incidentes.

Fuentes de información	▪ hxxps://10news.org/2022/05/conti-amenaza-con-cortar-el-agua-y-la-luz/ ▪ hxxps://www.americaeconomia.com/tecnologia-innovacion/ciberataque-conti-costa-rica

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 128**	**Fecha: 12-05-2022**
		Página 6 de 8

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	HP lanzó parches de seguridad para varios de sus productos		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. Resumen:

La empresa Hewlett-Packard (HP), ha lanzado múltiples parches de seguridad que corrigen dos vulnerabilidades de severidad ALTA que afectan el firmware UEFI de más de 200 computadoras portátiles, estaciones de trabajo y otros productos. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto la ejecución de código arbitrario en los dispositivos afectados.

2. Detalles:

- HP indicó que las vulnerabilidades han sido identificadas como CVE-2021-3808 y CVE-2021-3809, estas vulnerabilidades están relacionados con un controlador SMI (Interrupción de administración del sistema) que llama desde el Modo de administración del sistema (SMM), un modo de ejecución altamente privilegiado de los procesadores x86. El controlador SMI "puede activarse desde un contexto de ejecución del kernel, como un controlador del kernel de Windows", lo que permitiría a un atacante encontrar la dirección de memoria de una función específica y sobrescribirla en la memoria física para que apunte al atacante.
- Estas vulnerabilidades podrían permitir que un atacante se ejecute con privilegios de nivel de kernel (CPL == 0) para escalar los privilegios al modo de administración del sistema (SMM). Ejecutar en SMM le da al atacante privilegios completos sobre el host para llevar a cabo más ataques.
- HP indicó, que, han identificado posibles vulnerabilidades de seguridad en el BIOS (firmware UEFI) para ciertos productos de PC HP, lo que podría permitir la ejecución de código arbitrario.
- Estas vulnerabilidades afectan a numerosas computadoras portátiles y de escritorio comerciales, así como estaciones de trabajo de escritorio, dispositivos de puntos de venta minoristas y computadoras de cliente ligero.

3. Productos afectados:

- Computadoras portátiles, estaciones de trabajo y otros productos HP;
- Ver lista completa de dispositivos y equipos afectados.

4. Solución:

- HP recomienda instalar los parches de seguridad que corrigen estas vulnerabilidades. Asimismo, indicó que está lanzando actualizaciones de firmware para mitigar estas posibles vulnerabilidades en otros dispositivos afectados.
- De igual forma, dijo que los parches de seguridad de terceros que se van a instalar en los sistemas que ejecutan productos de software de HP deben aplicarse de acuerdo con la política de administración de parches del cliente.

Fuentes de información	▪ hxxps://support.hp.com/us-en/document/ish_6184733-6184761-16/hpsbhf03788 ▪ hxxps://nstarke.github.io/uefi/smm/2022/05/10/smm-callout-in-hp-products.html ▪ hxxps://www.securityweek.com/hp-patches-uefi-vulnerabilities-affecting-over-200-computers

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 128	Fecha: 12-05-2022
		Página 7 de 8

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad de omisión de restricciones de seguridad en PostgreSQL		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. Resumen:

Se ha reportado una vulnerabilidad de severidad MEDIA de tipo permisos, privilegios y controles de acceso en múltiples versiones de PostgreSQL. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto autenticado eludir las restricciones de seguridad implementadas y escalar privilegios dentro de la aplicación.

2. Detalles:

- La vulnerabilidad de permisos, privilegios y controles de acceso en múltiples versiones de PostgreSQL se debe a que los puntos débiles de esta categoría están relacionados con la gestión de permisos, privilegios y otras características de seguridad que se utilizan para realizar el control de acceso.
- La vulnerabilidad identificada como CVE-2022-1552 podría permitir a un usuario remoto eludir las restricciones de seguridad implementadas. La vulnerabilidad existe debido a restricciones de seguridad impuestas incorrectamente en Autovacuum, REINDEX, CREATE INDEX, REFRESH MATERIALIZED VIEW, CLUSTER y pg_amcheck. Un usuario remoto autenticado con permiso para crear objetos no temporales puede ejecutar funciones SQL arbitrarias bajo una identidad de super-usuario y escalar privilegios dentro de la aplicación.
- Un atacante tendría que enviar una solicitud especialmente diseñada a la aplicación afectada para aprovechar esta vulnerabilidad.

3. Productos afectados:

- PostgreSQL versión: 10.0, 10.1, 10.2, 10.3, 10.4, 10.5, 10.6, 10.7, 10.8, 10.9, 10.10, 10.10.4, 10.11, 10.12, 10.13, 10.14, 10.15, 10.16, 10.17, 10.18, 10.19, 10.20, 11.0, 11.0, 11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 11.7, 11.8, 11.9, 11.10, 11.11, 11.12, 11.13, 11.14, 11.15, 12, 12.0, 12.1, 12.2, 12.3, 12.4, 12.5, 12.6, 12.7, 12.8, 12.8, 12.9, 12.10, 13.0, 13.1, 13.2, 13.3, 13.4, 13.5, 13.6, 14.0, 14.1 y 14.2.

4. Solución:

- Se recomienda instalar PostgreSQL a la versión: 10.21, 11.16, 12.11, 13.7 y 14.3.

Fuentes de información	▪ hxxp://www.postgresql.org/about/news/postgresql-143-137-1211-1116-and-1021-released-2449/

Índice alfabético