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

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Asociación de Bancos del Perú

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

222-2024-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 Aéreadel 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 lasempresas 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°222	Fecha: 25-09-2024
		Página: 4 de 9

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	El ransomware DragonForce expande su RaaS y ataca a empresas de todo el mundo		
Tipo de Ataque	Ransomware	Abreviatur	Ransomware
Medios de propagación	Correo electrónico, redes sociales, entre otros		
Código de familia	C	Código de Sub familia	C01
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

El panorama del ransomware ha visto una gran fragmentación en los últimos dos años, con grandes grupos que cerraron después de convertirse en el blanco de acciones de aplicación de la ley o después de que atrajeron demasiada atención y tuvieron rescates puestos en las identidades de sus líderes.

Las operaciones de ransomware como servicio (RaaS) dependen en gran medida de piratas informáticos externos, conocidos como afiliados, para introducirse en las redes de las víctimas, robar datos y desplegar sus programas de cifrado de archivos. Estos afiliados ganan un gran porcentaje de los rescates pagados por las víctimas, por lo que existe una competencia constante entre las diferentes operaciones de ransomware para atraer a los afiliados con mejores acuerdos de comisiones o la promesa de una mayor seguridad operativa.

2. DETALLES:

El grupo de ransomware DragonForce surgió en agosto de 2023 y lanzó una variante basada en LockBit 3.0, una cepa de ransomware conocida. Sin embargo, en julio de 2024, el grupo introdujo una segunda variante, que inicialmente se afirmó que era su creación original, pero que luego se descubrió que era una bifurcación del ransomware ContiV3. Estas versiones duales de ransomware se utilizan para explotar vulnerabilidades en empresas, particularmente en sectores como la fabricación, el sector inmobiliario y el transporte.

DragonForce se considera un recién llegado al espacio del ransomware que se hizo un nombre en 2024 y está ascendiendo rápidamente en las filas. El grupo es conocido por tácticas de extorsión inusuales, como llamar a las víctimas y luego publicar las grabaciones en línea.

La estrategia de ataque de DragonForce se basa en una doble extorsión: encriptar los datos y amenazar con filtrarlos a menos que se pague un rescate. Esto añade una enorme presión a las víctimas para que cumplan, por temor no solo a una interrupción operativa, sino también al daño a la reputación que podría derivar de la exposición de información confidencial.

Los atacantes de DragonForce utilizan el phishing, así como credenciales RDP y VPN comprometidas para el acceso inicial a las redes.

Las operaciones de la banda de ransomware DragonForce son altamente personalizables, lo que permite a los afiliados configurar ataques según el tipo de víctima.

Con su programa de afiliados RaaS, lanzado el 26 de junio de 2024, el ransomware DragonForce ofrece a los atacantes la posibilidad de personalizar las cargas útiles del ransomware. Los afiliados pueden desactivar funciones de seguridad, establecer parámetros de cifrado e incluso personalizar las notas de rescate. A cambio, los afiliados reciben el 80% de cualquier rescate cobrado.

DragonForce emplea una variedad de técnicas avanzadas de evasión y persistencia. Una de sus tácticas clave es “Bring Your Own Vulnerable Driver” (BYOVD), donde los afiliados usan controladores vulnerables para deshabilitar procesos de seguridad y evadir la detección. Además, borran los registros de eventos de Windows después del cifrado para obstaculizar las investigaciones forenses.

Para el movimiento lateral, el grupo utiliza herramientas como Cobalt Strike y SystemBC , que les permiten recolectar credenciales y persistir en las redes. También utilizan herramientas de escaneo de redes como SoftPerfect Network Scanner para mapear las redes, lo que ayuda a propagar el ransomware a la mayor cantidad posible de dispositivos.

Además de utilizar las variantes ContiV3 y LockBit, la capacidad de DragonForce para adaptarse a las nuevas demandas de sus afiliados los convierte en una amenaza en rápido crecimiento. Al dirigirse a empresas con altos ingresos y sectores críticos, continúan aumentando su presencia en la infraestructura del cibercrimen.

3. RECOMENDACIONES:

- Ejecutar la estrategia 3-2-1-1-0 de copias de seguridad, que consiste en realizar periódicamente tres copias de seguridad de los datos, en mínimo dos medios de almacenamiento diferentes, y albergar una de las copias fuera del sitio o en la nube; además una de las copias esté disponible fuera de conexión, y cero copias sin verificar o con errores.
- Cifrar las copias realizadas. Así, incluso si se ven comprometidas, serían indescifrables e inútiles para el atacante.
- Aplicar parches y actualizar periódicamente el software y las aplicaciones a su última versión, así como realizar evaluaciones de vulnerabilidad periódicas.
- Utilizar un software antimalware confiable en sus dispositivos y mantenerlos actualizados. Estos programas pueden detectar y eliminar ransomware y otro software malicioso antes de que puedan cifrar sus archivos.
- Evitar abrir archivos adjuntos o enlaces sospechosos en correos electrónicos no solicitados o mensajes de redes sociales.
- Habilitar la autenticación de dos factores cuando esté disponible.
- Implementar el principio del privilegio mínimo para minimizar el impacto potencial de las infecciones de ransomware
- Habilitar la protección de red para evitar que las aplicaciones o los usuarios accedan a dominios y otro contenido maliciosos en Internet.
- Implementar soluciones de seguridad avanzadas, como sistemas de detección y respuesta de endpoints (EDR), y software de detección y prevención de intrusiones (IDS/IPS), para identificar y bloquear comportamientos sospechosos antes de que causen daños significativos.
- Centrar la estrategia de defensa en la detección de movimientos laterales y el bloqueo de actividades fraudulentas de transferencia de datos confidenciales a Internet (fuga de informaciones). Es importante prestar especial atención al tráfico saliente para detectar las conexiones de los ciberdelincuentes en su red.
- Capacitar a su equipo en las mejores prácticas de ciberseguridad y manténgalos informados sobre las últimas amenazas.

Fuente de Información:	• hxxps://hackread.com/dragonforce-ransomware-expands-raas-targets-firms/ • hxxps://www.computerworld.es/article/3530957/los-10-principales-grupos-de-ransomware-que-hay-que-tener-en-el-radar.html

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°222	Fecha: 25-09-2024 Página: 6 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de escalada de privilegios en varios productos de Cisco		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Cisco ha publicado una vulnerabilidad de severidad **ALTA** de tipo autorización indebida que afecta a varios de sus productos. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto autenticado realizar modificaciones no autorizadas en la configuración de la aplicación o dispositivo afectado, incluida la creación de nuevas cuentas de usuario o la elevación de sus propios privilegios en un sistema afectado.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-20381 de tipo autorización indebida en la función API JSON-RPC en Cisco Crosswork Network Services Orchestrator (NSO) y ConfD que es utilizada por las interfaces de administración basadas en web de Cisco Optical Site Manager y Cisco RV340 Dual WAN Gigabit VPN Routers, podría permitir que un atacante remoto autenticado modifique la configuración de una aplicación o dispositivo afectado. Esta vulnerabilidad también afecta a ConfD si la función API JSON-RPC está habilitada.

Esta vulnerabilidad se debe a comprobaciones de autorización incorrectas en la API. Un atacante con privilegios suficientes para acceder a la aplicación o dispositivo afectado podría aprovechar esta vulnerabilidad enviando solicitudes maliciosas a la API JSON-RPC. Una explotación exitosa podría permitir al atacante realizar modificaciones no autorizadas en la configuración de la aplicación o dispositivo afectado, incluida la creación de nuevas cuentas de usuario o la elevación de sus propios privilegios en un sistema afectado.

A. Productos afectados:

Esta vulnerabilidad afecta a los siguientes productos de Cisco si utilizan la configuración predeterminada inicial con la interfaz de usuario web habilitada:

- Crosswork NSO, versiones anteriores a la 6.3.
- Optical Site Manager, versiones anteriores a la 24.3.
- RV340 Dual WAN Gigabit VPN Routers.

3. RECOMENDACIÓN:

- Actualizar los paquetes afectados a la última versión disponible que Cisco ha lanzado para abordar esta vulnerabilidad. No existen soluciones alternativas.

Fuente de Información:	• hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nso-auth-bypass-QnTEesp

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°222	Fecha: 25-09-2024 Página: 7 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en productos Apple		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Apple ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo autorización incorrecta en varios de sus productos. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado eludir los mecanismos de autenticación, lo que daría lugar a un acceso no autorizado a información y sistemas confidenciales.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2024-6592 de tipo autorización incorrecta en la comunicación de protocolo entre WatchGuard Authentication Gateway (también conocido como Single Sign-On Agent) en Windows y WatchGuard Single Sign-On Client en Windows y MacOS. Esta vulnerabilidad permite que un atacante con acceso a la red falsifique las comunicaciones con los componentes afectados.

Un atacante podría eludir los mecanismos de autenticación, lo que daría lugar a un acceso no autorizado a información y sistemas confidenciales. Esto podría dar lugar a violaciones de datos, modificaciones no autorizadas del sistema o un mayor compromiso de la infraestructura afectada. Esta vulnerabilidad se puede explotar a través de la red sin necesidad de interacción o privilegios del usuario.

A. Productos afectados:

- WatchGuard Authentication Gateway, versiones hasta la 12.10.2 en Windows.
- WatchGuard Single Sign-On Client: versiones hasta la 12.7 en Windows.
- WatchGuard Single Sign-On Client: versiones hasta la 12.5.4 en MacOS.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad.
- Usar reglas de Firewall de Windows para restringir el acceso a la red del puerto TCP 4116 al cliente de inicio de sesión único para permitir únicamente conexiones desde la puerta de enlace de autenticación (agente SSO) y restringir el acceso a la red del puerto TCP 4114 a la puerta de enlace de autenticación para permitir únicamente conexiones desde Firebox.
- Usar objetos de política de grupo para agregar reglas de firewall de Windows a sus puntos finales.
- Implementar la segmentación de la red para limitar el potencial impacto de una explotación exitosa.
- Supervisar cualquier intento de autenticación sospechoso o acceso no autorizado.
- Implementar controles de acceso sólidos y autenticación multifactor cuando sea posible para agregar una capa adicional de seguridad.
- Auditar y revisar periódicamente los registros de autenticación para detectar cualquier signo de compromiso.

Fuente de Información:	• hxxps://www.watchguard.com/wgrd-psirt/advisory/wgsa-2024-00014 • hxxps://www.redteam-pentesting.de/advisories/rt-sa-2024-006

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°222	Fecha: 25-09-2024
		Página: 8 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en el protocolo Pragmatic General Multicast del kernel de Microsoft Windows		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Se ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo de corrupción de memoria en el protocolo Pragmatic General Multicast (PGM) del kernel de Microsoft Windows 10. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto enviar paquetes de red especialmente diseñados y obtener acceso a una estructura de memoria obsoleta, lo que provocaría la corrupción de la memoria.

2. DETALLES:

PGM es un protocolo de transporte de multidifusión basado en IP que está estandarizado como RFC3208. Este protocolo es implementado por Microsoft como parte del servicio Microsoft Message Queueing que está disponible en diferentes versiones del sistema operativo Windows. El protocolo PGM tiene como objetivo proporcionar un mecanismo mediante el cual los miembros de un grupo de multidifusión puedan detectar mensajes perdidos o desordenados y tomar medidas correctivas para garantizar la entrega confiable de cada paquete que compone un flujo de mensajes. El protocolo PGM también ofrece soporte explícito para la corrección de errores de reenvío mediante codificación Reed-Solomon.

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2024-38140 de tipo corrupción de memoria en el protocolo Pragmatic General Multicast del kernel de Microsoft Windows 10, podría permitir a un atacante remoto enviar paquetes de red especialmente diseñados y obtener acceso a una estructura de memoria obsoleta, lo que provocaría la corrupción de la memoria. Un atacante puede enviar una secuencia de paquetes maliciosos para activar esta vulnerabilidad.

A. Productos afectados:

- Microsoft Pragmatic General Multicast 10.0.19041.4474.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.

Fuente de Información:	• hxxps://www.talosintelligence.com/vulnerability_reports/TALOS-2024-2062 • hxxps://www.microsoft.com/en-us/research/wp-content/uploads/2003/03/pgm_ieee_network.doc • hxxps://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38140

Índice alfabético