UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS “ESPOG”

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: RPC-SO-02-No.053-2021

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER

Título del artículo
GUÍA DE ANÁLISIS DE BRECHAS DE SEGURIDAD PARA ENTORNOS DE HIPERVISORES
Línea de Investigación:
SEGURIDAD INFORMÁTICA
Campo amplio de conocimiento:
TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN
Autor:
Christian Bolívar Gavilanes Quiroga
Tutor:
MSc. Pablo Marcel Recalde Varela

Quito – Ecuador

2023

APROBACIÓN DEL TUTOR

Yo, Pablo M Recalde V con C.I: 1711685055 en mi calidad de Tutor del proyecto de investigación titulado: **Guía de análisis de brechas de seguridad para entornos de hipervisores**.

Elaborado por: Christian Bolívar Gavilanes Quiroga, de C.I: 1716298136, estudiante de la Maestría: Seguridad Informática de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., marzo de 2023

Firma

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Universidad Israel

Yo, Christian Bolívar Gavilanes Quiroga con C.I: 1716298136, autor del proyecto de titulación denominado: Guía de análisis de brechas de seguridad para entornos de hipervisores. Previo a la obtención del título de Magister en Seguridad Informática.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., marzo de 2023

Firma

ORCID: 0000-0003-3888-7877

TABLA DE CONTENIDOS

Índice de Tablas

Índice de Figuras

Información General

Contextualización del problema

El avance tecnológico de los últimos años ha crecido de una manera significativa por tal motivo gran parte de las empresas se vieron en la necesidad de acoplarse a este avance tecnológico, por tal motivo han evolucionado sus infraestructuras para poder soportar los servicios que brindan.

Según IONOS Digital Guide. (2019) La virtualización de los sistemas es primordial para el desarrollo de infraestructuras dentro de las organizaciones. En estos entornos las partes interesadas (clientes y proveedores) cuestiona la seguridad en varios niveles y como consecuencia la seguridad de la virtualización de los sistemas subyacentes, como son los niveles de servicios (SLA), acceso a los recursos y la restricción de acceso a datos no autorizados, para garantizar la confidencialidad e integridad de los recursos.

La virtualización ha realizado esfuerzos para mejorar el rendimiento con la aparición de nuevas tecnologías, y hace referencia para la creación de máquinas virtuales a través de la virtualización del hardware, software, almacenamiento, red y datos.

La implementación de estos modelos de virtualización podría verse afectada por ataques de ciberdelincuentes y provocar el aislamiento de los hipervisores, los mismos que se intercomunican entre las capas verticales de su estructura y sería extremadamente difícil de establecer una seguridad de defensa profunda.

Problema de Investigación

«No existe un mayor esfuerzo para el manejo de riesgos y seguridad al momento de la implementación de hipervisores. Los riesgos de seguridad deben ser el punto más importante que se debe considerar para el desarrollo y correcto funcionamiento en un entorno virtualizado, lamentablemente no se los toman en consideración y prevalecen las vulnerabilidades» Arévalo (2021).

Según Bhagat et al. (2020), los autores demostraron que los sistemas operativos, la mala configuración y aplicaciones instaladas son las fuentes principales de vulnerabilidades. Por ejemplo, los puertos abiertos que no son utilizados, el uso de cuentas y contraseñas predeterminadas, autenticación y autorización débiles, la habilitación o instalación de funciones innecesarias. Esta mala configuración es uno de los factores principales detrás de los ataques a un hipervisor.

¿Con la identificación oportuna de vulnerabilidades en los hipervisores, se puede identificar brechas de seguridad para establecer mecanismos de control y seguridad?

Objetivo general

- Desarrollar una guía que permita elegir una estrategia para la protección de los hipervisores en entornos virtualizados.

Objetivos específicos

- Analizar las vulnerabilidades a las que están expuestos los hipervisores.
- Categorizar las vulnerabilidades identificadas previamente, mediante estrategias de protección de la información.
- Comparar las metodologías Magaret, Octane, Zero Trust que existen para modelos de seguridad.
- Especificar las acciones apropiadas para la protección de los activos con la implementación de la metodología mejor se adapte.

Vinculación con la sociedad y beneficiarios directos

El análisis de la metodología permitirá a las personas del área de informática implementar políticas y controles para proteger la información que se encuentra almacenada en los entornos virtualizados.

CAPÍTULO I: DESCRIPCIÓN DEL ARTÍCULO PROFESIONAL

Las empresas consideran a la virtualización la mejor alternativa para el crecimiento de sus negocios, debido a que no se requiere una gran cantidad de infraestructura y los costos son más accesibles. No obstante, estas tecnologías son vulnerables a ataques informáticos los mismos que pueden provocar pérdidas de información.

1.1 Contextualización general del estado del arte

Según el sitio web VMWARE (2023), «La virtualización inició en la década de 1960, cuando la empresa IBM tuvo la intención de segmentar los centros de cómputos o mainframes para mejorar el uso de recursos de la unidad de procesamiento, dio como resultado la generación de un mainframe que puede realizar varias operaciones en forma simultánea. Al comienzo del año 1980 y 1990, con la aparición de la arquitectura x86 ésta, se convirtió en la arquitectura seleccionada, mientras que la computación se volvía distribuida y tomaba fuerza en la industria de Tecnologías de Información (TI). El incremento de la arquitectura x86 causó una migración masiva en la virtualización y el modelo cliente-servidor comenzó un aumento en su popularidad de forma acelerada.

En los años de 1960 IBM inició con la implementación de diferentes particiones lógicas en un solo equipo con el fin de la optimización de recursos. El primer computador diseñado específicamente para la virtualización fue mainframe IBM Modelo 67, con un sistema operativo que IBM llamó S.O. de supervisor o VMM (virtual machine monitor) hasta que fue evolucionando y convirtiéndose en lo que hoy en día se conoce como Hipervisor.

Existen diferentes tipos de virtualización:

Virtualización de servidor o por hardware

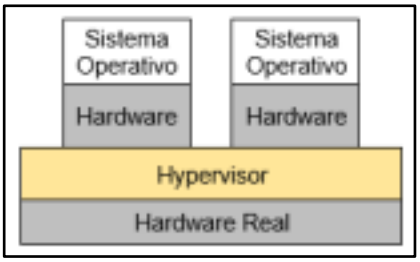
Según Castillo, (2018) Este método es el más común y utilizado en los entornos de servidores dentro de las empresas. El procedimiento consiste en la creación de uno o varios servidores virtuales asignando actividades específicas. Este procedimiento consiste en la creación de diferentes servidores virtuales, que utilicen la mínima cantidad de recursos dentro de un servidor físico de mayor tamaño y con un hardware más potente. De esta forma las máquinas se encuentren independientes unas de otras y se distribuyen los recursos de hardware para funcionar de forma eficiente.

Se asigna un Hipervisor para ejecutar los controles de los elementos como procesadores, memoria RAM, los discos duros y demás componentes para la asignación de varios sistemas operativos de forma virtual que se ejecutarán de forma simultánea dentro de una máquina. Esto marcó un antes y un después dentro de las empresas que se dedican a proporcionar servicios de hosting y otros tipos de servicios a otras empresas.

Ahorro en hardware: Solo se destina los recursos económicos en la adquisición de un solo equipo con el hardware necesario para la virtualización.

Escalabilidad: Permite la creación de nuevos equipos virtuales sin la necesidad de adquirir nuevos elementos físicos.

Figura 1:
Virtualización por Hardware

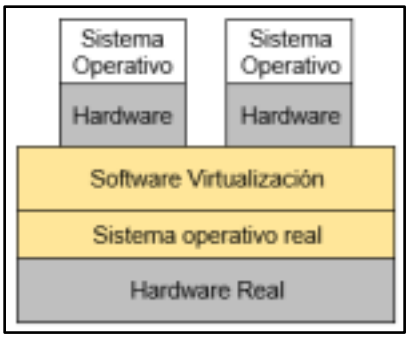


Nota*:* Por el autor

Virtualización a nivel de sistema operativo

Según Limones, (2021) Este tipo de virtualización, ya no es necesario la existencia de un sistema operativo para cada instancia, sino se dispone un servidor físico con un único sistema operativo, y en él mismo se van creando las instancias (aisladas entre sí) cada una contiene una réplica del sistema operativo principal (el kernel es fundamental para que esto sea posible).

Figura 2:
Virtualización por sistema operativo

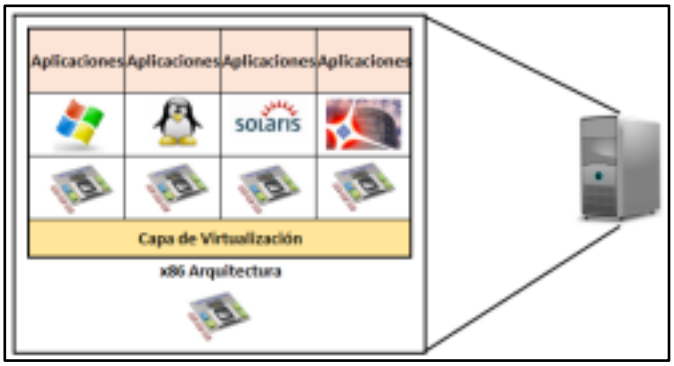


Nota*:* Por el autor

Virtualización de aplicaciones

La ejecución de la virtualización de aplicaciones se realiza de forma independiente en el sistema operativo, esta solución es la adecuada para cuando se tienen aplicaciones que no son compatibles entre ellas. Este tipo de virtualización convierte las aplicaciones en servicios virtualizados, con la administración centralizada y que no requieren estar instalados, por este motivo no presentaran conflictos con las demás aplicaciones.

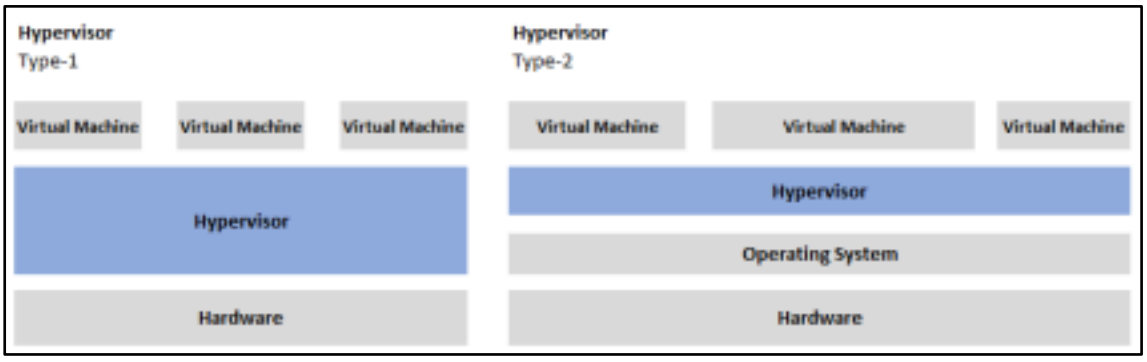
Figura 3:
Virtualización de aplicaciones



Nota*:* Por el autor

Lo anterior presentó los diferentes modelos de virtualización, incluida la virtualización que se basa en hipervisores tipo I y Tipo II, esta arquitectura se detalla en la Figura 4 que representa los modelos de virtualización, la cual nos servirá para el análisis de seguridad.

Figura 4:
Hipervisores Tipo I y Tipo II



Nota: Por el autor

Análisis de seguridad basada en la arquitectura de referencia.

Se realizó el análisis de seguridad basado en la arquitectura de referencia. Primero, se investigó las vulnerabilidades con la ayuda de los Common Vulnerabilities and Exposures (CVE) y de investigación realizada por Compastié (2020), se clasificó y evaluó cualitativamente la criticidad de las vulnerabilidades (en términos de ocurrencias) con respecto a los modelos de virtualización. Luego se determinaron las amenazas que afectan a la arquitectura para identificar las vulnerabilidades.

Aplicaciones de máquina virtual.

Las vulnerabilidades generalmente se encuentran relacionadas con la gestión de la memoria, con respecto a la verificación del tipo de variable en tiempo de ejecución, la desasignación de memoria, la inferencia del kernel en el espacio del usuario y las fallas del software de desarrollo y con las interfaces de software, con respecto al control de acceso, posible inyección de código, y concurrencia.

Máquina Virtual Guest

Las vulnerabilidades se relacionan con la administración del software, incluida la resolución de dependencias, la degradación del servicio y los problemas de configuración y la supervisión del kernel del sistema operativo (incluida la criticidad del kernel, los mecanismos de seguridad específicos, el acceso al espacio del usuario y la exposición del hardware).

Hipervisor

Los hipervisores están expuestos a una gran cantidad de vulnerabilidades relacionadas con las diafonías entre máquinas virtuales, como la infraestructura de red compartida y otros problemas de uso compartido de recursos, las diafonías entre máquinas virtuales e hipervisores, como el uso compartido de recursos con el host, la implementación de virtualización y el hipervisor. Problemas de supervisión y la consola de administración, como la supervisión del hipervisor y los problemas de ejecución de máquinas virtuales no lineales.

Entorno de ejecución de hipervisor

Está basado en el sistema operativo host o hardware, de los hipervisores también se ve afectado por diferentes vulnerabilidades relacionadas con el sistema operativo host y el hardware.

En la tabla 1 se muestra el análisis de vulnerabilidades por entorno y componente.

Tabla 1:
Análisis de Vulnerabilidades

Entorno	Componente	Descripción de la vulnerabilidad	Hipervisor TIPO I	Hipervisor TIPO II
Aplicaciones de máquina virtual	Gestión de memoria	Comprobación de tipos de variables en tiempo de ejecución	●	●
		Desasignación de memoria	●	●
		Inferencia del kernel en el espacio de usuario	⊖	⊖
	Interfaces de software	Fallo del software de desarrollo	●	●
		Control de acceso	●	●
		Inyección de código	●	●
		concurrencia	⊖	⊖
Máquina Virtual Guest OS	Gestión de software	Error de resolución de dependencia	●	●
		grado de servicio durante la gestión	⊖	⊖
		Problema de configuración	●	●
	Supervisión del kernel del sistema operativo	Criticidad del núcleo	⊖	⊖
		Inaplicable seg. Mecánico	●	●
		Acceso al espacio de usuario	●	●
		Exposición de hardware	●	●
	Diafonía entre máquinas virtuales	Co-residencia	⊖	⊖
		Redes compartidas	⊖	⊖
		Otros recursos compartidos	⊖	⊖
Hipervisor	Diafonía de VM-hipervisor	Compartir recursos con el anfitrión	⊖	⊖
		Implementación del método de virtualización	⊖	⊖
	Administración de consola	Supervisión del hipervisor	⊖	⊖
		Supervisión de la consola de administración	⊖	⊖
		Ejecución de máquina virtual no lineal/no monótona	⊖	⊖
Entorno de ejecución de hipervisor	Host	sistema operativo Local	⊖	⊖
	Hardware	Vigilancia	⊖	⊖
		Propiedad física	⊖	⊖
		Actualizaciones	⊖	⊖
		Acceso físico	⊖	⊖

Nota: Representa respectivamente, ⊖ Medio, ● Alto

En la tabla 2, se muestran los detalles de vulnerabilidades analizadas de los CVE con su categorización.

Tabla 2:
CVE de vulnerabilidades hasta febrero de 2023

CVE	Tipo de Vulnerabilidad	Descripción	Tipo de Acceso	Complejidad	Score	Hipervisor Tipo 1	Hipervisor Tipo 2
CVE-2022-35867	Escalada de Privilegio	La vulnerabilidad permite al atacante local incrementar privilegios en los sistemas afectados. El atacante obtendrá primeramente la capacidad de ejecución de código con privilegios elevados en los sistemas del invitado de destino. La falla específica existe dentro del dispositivo virtual e1000. Este problema se da por falta de las validaciones adecuadas en la longitud de datos que son proporcionados por los usuario antes de ser ingresados en el búfer tipo pila. Los atacantes pueden aprovechar de esta vulnerabilidad para aumentar los privilegios y poder ejecutar los códigos arbitrarios en el hipervisor. Era ZDI-CAN-1505	Remoto	Medio	6.7	X	X
CVE-2022-34889	Escalada de Privilegio	La vulnerabilidad permite al atacante local incrementar privilegios en las sistemas afectados de Parallels Desktop 17.1.1 (51537). el atacante obtendrá primeramente la capacidad de ejecución de código con privilegios incrementados en los sistemas del invitado de destino para aprovecharse de la vulnerabilidad. La falla específica existe dentro del dispositivo virtual ACPI. El problema es por falta de las validaciones adecuadas en los datos que proporciona el usuario, lo que puede resultar en una lectura más allá del final de un búfer asignado. los atacantes pueden ejecutar códigos de forma arbitraria en el hipervisor. Era ZDI-CAN-16554.	Remoto	Alto	8.2	X	X
CVE-2022-32295	Exec Code Overflow	En los dispositivos Ampere Altra y AltraMax anteriores a SRP 1.09, el diseño de referencia de Altra de los accesos UEFI permite el acceso inseguro a SPI-NOR por parte del componente OS/hipervisor.	Local	Alto	9.8	X	
CVE-2022-25681	Memoria	Posible corrupción de la memoria en el kernel al realizar el acceso a la memoria debido a que el hipervisor no invalidó correctamente las cachés de traducción del procesador en Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	Local	Alto	7.8	X	X

CVE	Tipo de Vulnerabilidad	Descripción	Tipo de Acceso	Complejidad	Score	Hipervisor Tipo 1	Hipervisor Tipo 2
CVE-2022-23034	Escritura fuera de límites	Un invitado de PV podría DoS Xen mientras desasigna una concesión Para abordar XSA-380, se introdujo el recuento de referencias para las asignaciones de concesión en el caso de que un invitado de PV tuviera IOMMU habilitado. Los huéspedes de PV pueden solicitar dos formas de asignaciones. Cuando ambos están en uso para cualquier asignación individual, se puede solicitar la eliminación de dicha asignación en dos pasos. El recuento de referencia para tal mapeo se reduciría dos veces por error. Se detecta el subdesbordamiento de los contadores, lo que provoca la activación de una comprobación de errores del hipervisor.	Remoto	Medio	5.5	X	X
CVE-2022-23030	Escritura fuera de límites	En la versión 16.1.x anterior a la 16.1.2, 15.1.x anterior a la 15.1.4.1, 14.1.x anterior a la 14.1.4.5 y todas las versiones de 13.1.x, cuando BIG-IP Virtual Edition (VE) usa el controlador ixlv (que se usa en modo SR-IOV y requiere la familia de adaptadores de red Intel X710/XL710/XXV710 en el hipervisor) y la configuración de descarga de segmentación TCP está habilitada, las solicitudes no reveladas pueden causar un aumento en la utilización de recursos de la CPU. Nota: No se evalúan las versiones de software que han llegado al final del soporte técnico (EoTS).	Remoto	Medio	5.3	X	X
CVE-2022-22093	Memoria	Corrupción de la memoria o denegación temporal del servicio debido al manejo inadecuado de operaciones simultáneas de hipervisor para adjuntar o desconectar IRQ de fuentes de interrupción virtual en Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	Local	Alto	7.0	X	X
CVE-2022-21816	Denegación de Servicio	El software NVIDIA vGPU contiene una vulnerabilidad en Virtual GPU Manager (nvidia.ko), donde un usuario en el sistema operativo invitado puede provocar una tormenta de interrupción de GPU en el host del hipervisor, lo que lleva a una denegación de servicio.	Local	Bajo	5.5	X	X
CVE-2021-22045	Exec Code Overflow	Los sistemas VMware ESXi (7.0, 6.7 antes de ESXi670-202111101-SG y 6.5 antes de ESXi650-202110101-SG), VMware Workstation (16.2.0) y VMware Fusion (12.2.0) contienen una vulnerabilidad de desbordamiento de montón en la emulación de dispositivos de CD-ROM	Local	Medio	6.9	X	X

CVE	Tipo de Vulnerabilidad	Descripción	Tipo de Acceso	Complejidad	Score	Hipervisor Tipo 1	Hipervisor Tipo 2
CVE-2021-21995	Denegación de Servicio	OpenSLP como se usa en ESXi tiene una vulnerabilidad de denegación de servicio debido a un problema de lectura fuera de los límites del montón.	Remoto	Bajo	5	X	
CVE-2021-21994	Bypass	SFCB (Small Footprint CIM Broker) cómo se usa en ESXi tiene una vulnerabilidad de omisión de autenticación	Remoto	Medio	6.8	X	
CVE-2021-21974	Exec Code Overflow	OpenSLP como se usa en ESXi (7.0 antes de ESXi70U1c-17325551, 6.7 antes de ESXi670-202102401-SG, 6.5 antes de ESXi650-202102101-SG) posee como vulnerabilidad el desbordamiento en la pila	Red Local	Bajo	5.8	X	
CVE-2020-4005	Escalada de Privilegios	VMware ESXi (7.0 antes de ESXi70U1b-17168206, 6.7 antes de ESXi670-202011101-SG, 6.5 antes de ESXi650-202011301-SG) contiene una vulnerabilidad de escalada de privilegios que existe en la forma en que se administran ciertas llamadas al sistema	Local	Medio	7.2	X	
CVE-2020-4004	Exec Code	VMware ESXi (7.0 antes de ESXi70U1b-17168206, 6.7 antes de ESXi670-202011101-SG, 6.5 antes de ESXi650-202011301-SG), Workstation (15.x antes de 15.5.7), Fusion (11.x antes de 11.5.7) contiene un uso -vulnerabilidad after-free en el controlador USB XHCI.	Local	Bajo	4.6	X	X
CVE-2020-3992	Exec Code	OpenSLP como se usa en VMware ESXi (7.0 antes de ESXi_7.0.1-0.0.16850804, 6.7 antes de ESXi670-202010401-SG, 6.5 antes de ESXi650-202010401-SG) tiene un problema de uso después de la liberación	Remoto	Alto	10	X	

CVE	Tipo de Vulnerabilidad	Descripción	Tipo de Acceso	Complejidad	Score	Hipervisor Tipo 1	Hipervisor Tipo 2
CVE-2020-3982	Escritura fuera de límites	VMware ESXi (7.0 antes de ESXi_7.0.1-0.0.16850804, 6.7 antes de ESXi670-202008101-SG, 6.5 antes de ESXi650-202007101-SG), Workstation (15.x), Fusion (11.x antes de 11.5.6) contienen una salida Vulnerabilidad de escritura fuera de los límites debido a un problema de tiempo de uso en el dispositivo ACPI. Un actor malicioso con acceso administrativo a una máquina virtual puede aprovechar esta vulnerabilidad para bloquear el proceso vmx de la máquina virtual o dañar el montón de memoria del hipervisor.	Remoto	Bajo	4.9	X	X
CVE-2020-3981	Escritura fuera de límites	VMware ESXi (7.0 antes de ESXi_7.0.1-0.0.16850804, 6.7 antes de ESXi670-202008101-SG, 6.5 antes de ESXi650-202007101-SG), Workstation (15.x), Fusion (11.x antes de 11.5.6) contienen una salida Vulnerabilidad de lectura fuera de los límites debido a un problema de tiempo de uso en el dispositivo ACPI	Remoto	Bajo	3.5	X	X
CVE-2020-3976	DoS	VMware ESXi y vCenter Server contienen una vulnerabilidad de denegación de servicio parcial en sus respectivos servicios de autenticación	Remoto	Bajo	5	X	X

Fuente: Autoría propia, basado en los Common Vulnerabilities and Exposures

1.2 Proceso investigativo metodológico

Para el desarrollo del trabajo se ha utilizado un proceso de investigación cualitativa exploratorio con la revisión de artículos de investigación, tesis, determinando como los métodos de seguridad de tecnología servirá de guía y permita elegir una estrategia para la protección en los hipervisores.

Análisis de amenazas y ataques

«Utilizando las metodologías de modelos de seguridad para analizar las amenazas y ataques que se relacionan con la arquitectura de referencia, se considera un conjunto principal de amenazas, suplantación de identidad, manipulación, repudio, divulgación de información, denegación de servicio y elevación de privilegios.» (Shashank Guptah, 2017).

Se detalla en la tabla 3 el objetivo de estos ataques, principalmente en máquinas virtuales e hipervisores que son objetivos de un atacante.

Tabla 3:
Relación de amenazas y ataques a la arquitectura en referencia

		Suplantación de identidad	**Manipulación**	**Repudio**	**Divulgación de información**	**Negación de servicio**	**Elevación de privilegio**
Hipervisor TIPO 1-2	Máquina Virtual	Hyperjacking VM movilidad	Diseño Software defectuoso Exploits en software de aplicación VM Hopping VM Escape VM	Supervisión entre máquinas virtuales Supervisión de máquina virtuales y el host	Exploits en software de aplicación Supervisión entre máquinas virtuales Supervisión de máquina virtuales y el host	Denegación de servicios entre máquinas virtuales	Exploits en software de aplicación VM Hopping VM Escape VM
Hipervisor TIPO 1-2	Hypervisor		Explotación al canal de control Explotación al hipervisor Escape de la máquina virtual y el host	Explotación al canal de control Explotación al hipervisor	Explotación al hipervisor Cálculo de monopolización	Denegación de servicios al hipervisor	VM Escape VM
Hipervisor TIPO 2	Sistema Operativo		VM Escapto VM			Denegación de servicios de hipervisor	VM Escape VM
Hipervisor TIPO 1	Hardware		Explotación al Firmware		Explotación al Firmware	Denegación de servicios al hipervisor	Explotación al Firmware

Nota: Por el autor, basado en el artículo Shashank Guptah, 2017.

Los elementos críticos analizados servirán como guía al personal de seguridad en qué elementos deben tener mayor cuidado dentro de los entornos virtualizados.

- Las aplicaciones de máquinas virtuales (VM), crean instancias que exponen interfaces que se pueden acceder de forma remota, el atacante externo de forma remota puede usar las interfaces expuestas.
- La capa de hardware no es accesible para el atacante de forma remota, por lo que se considera una intrusión física fuera de la virtualización.
- Los activos a los que se dirige el atacante son aplicaciones y datos ubicados en máquinas virtuales VM.
- El objetivo de los atacantes es impactar de forma negativa en la disponibilidad (denegación de servicio), la integridad (alteración) o la confidencialidad (recuperación) de un activo.
- Los componentes se consideran seguros si no están comprometidos, pero los mismos pueden contener fallas en el software inherente que pueden ser conocidas por el atacante, el atacante las puede explotar para comprometer algún componente y obtener influencia o control sobre él.

Mecanismos de seguridad

Las contramedidas consisten en la protección de recursos o componentes y estos deben ser considerados al momento de diseñar e integrar los mecanismos de seguridad, estas contramedidas puede afectar tanto a las máquinas virtuales como al hipervisor.

Según Compastié (2020), la protección de recursos de la máquina virtual y hipervisores se los realiza en la integración de mecanismos de seguridad al momento de diseño de la máquina virtual y hipervisor.

Máquina Virtual

- Kernel del sistema operativo.
- Basado en Aplicaciones.
- Gestión de software seguro.

Hipervisor

- Entorno de ejecución
- Granularidad del hipervisor
- protección de Redes y Almacenamiento

Se detalla en la tabla 4 se detalla las contramedidas al momento de integración de mecanismos de seguridad en tiempo de diseño. A las máquinas virtuales y hipervisores

Tabla 4:
Contramedidas al momento de integración.

Mecanismo	Área de Protección	Contramedidas	Cobertura	Requisitos
Integración de Mecanismos de Seguridad en Tiempo de Diseño	Protección Máquina Virtual	Contador basado en la medida de kernel	kernel del sistema operativo, Kernel del sistema operativo host	Existencia de implementaciones de mecanismos para los núcleos operados
		Basado en aplicaciones	Solicitud, tiempo de ejecución	Existencia de implementaciones de mecanismos para todas las aplicaciones operadas y su tiempo de ejecución
		Gestión de software seguro	kernel del sistema operativo, Aplicación, tiempo de ejecución	Gestión de software seguro solo para los administradores de paquetes
		Entorno de ejecución	Hipervisor, Kernel del sistema operativo host	implementación de mecanismos en los hipervisores operados
	Protección Hipervisor	Granularidad del hipervisor	hipervisor	Arquitectura modular del hipervisor
		Protección de Redes y Almacenamiento	hipervisor	Dispositivos de almacenamiento y redes. Interfaces del hipervisor

Nota: Por el autor, basado en el artículo Compastié 2020

Para minimizar la superficie de ataque se debe enfocar en las técnicas de verificación y caídas de capacidades del recurso, esto nos permite evaluar las propiedades de seguridad en los componentes de la arquitectura y también verificar el diseño de los mecanismos de seguridad:

- Verificación formal de Código
- Reducción de procesos innecesarios en el Procesador
- Externalización de VM Gestión de software

Se detalla en la tabla 5 se detalla las contramedidas para minimizar la superficie de ataque:

Tabla 5:
Contramedidas para minimizar superficie de ataque.

Mecanismo	Contramedidas	Cobertura	Requisitos
Minimización de la superficie de ataque	Verificación formal de Código	Núcleo del sistema operativo, hipervisor, Kernel del sistema operativo host	Base de código, diseño y mantenibilidad limitados al momento de la ejecución de pruebas
	Reducción de procesos innecesarios en el Procesador	Todos los componentes de software	Diseño modular y soporte para deshabilitar características en tiempo de ejecución
	Externalización de VM Gestión de software	Aplicación, tiempo de ejecución, núcleo del sistema operativo	Instancia de máquina virtual de corta duración, imagen protegida en el entorno de construcción

Nota: Por el autor, basado en el artículo Compastié 2020

La adaptación basada en la programabilidad de seguridad como contramedida son eficientes en la reducción de la superficie de ataque, pero deben irse adaptando constantemente en el tiempo para enfrentarse a nuevas amenazas y ataques. La programabilidad de recursos y mecanismos de seguridad puede ser impulsado por una actividad que se base en los resultados de la supervisión.

Se detalla en la tabla 6 las contramedidas para la adaptación basada en la programabilidad de seguridad.

Tabla 6:
Contramedidas para programabilidad de seguridad.

Mecanismo	Contramedidas	Cobertura	Requisitos
Adaptación basada en Seguridad Programabilidad	Seguimiento de recursos compartidos	Aplicación, tiempo de ejecución, núcleo del sistema operativo	Existencia de interfaces para monitorear y conocimiento necesario para el monitore de datos
	Controles de Seguridad a los Mecanismos	Aplicación, tiempo de ejecución, núcleo del sistema operativo	Especificación de los requisitos de seguridad y características del mecanismo
	Programabilidad de seguridad	Aplicación, tiempo de ejecución, núcleo del sistema operativo	Interfaces de reconfiguración, o posibilidad de reiniciar componentes

Nota: Por el autor, basado en el artículo Compastié 2020

1.3 Análisis de resultados

Después de haber clasificado los ataques de seguridad con la ayuda de los modelos de riesgos, nos enfocamos principalmente en los ataques de máquinas virtuales VM e Hipervisores.

Máquina virtual.

Se consideran en esta categoría, los ataques de denegación de servicio de VM, que consisten en bloquear o interrumpir el correcto funcionamiento de una máquina virtual.

- Dependiendo el tipo de ataque puede o no puede tener control total sobre el recurso, permitiendo exfiltrar datos, afectando su disponibilidad. Este ataque se puede realizar desde el hipervisor, explotando la vulnerabilidad de supervisión de la consola de administración.
- Una forma más discreta de proceder con una denegación de servicio de este tipo es reconfigurar el entorno de hardware virtual para que la máquina virtual no funcione correctamente; por ejemplo, reduciendo la memoria RAM asignada, para reducir la huella del ataque.
- La red también se puede utilizar para realizar este tipo de ataques. Basado en la vulnerabilidad de la exposición del hardware en el sistema operativo, generando carga de trabajo masiva en la red el mismo que provoca que la máquina virtual no esté disponible.

Hipervisores

Estos ataques se relacionan a la denegación de servicios que están enfocados a los hipervisores.

- La consola de administración representa un vector de ataque, ya que puede apagar el hipervisor, vulnerabilidad de supervisión de la consola de administración.
- Los protocolos de red se pueden utilizar para inundar el hipervisor o su entorno de ejecución en función de los ataques DDoS.
- Los hipervisores también están compuestos por componentes de software, que tienen sus propias vulnerabilidades que los atacantes pueden aprovechar.

Comparativa de modelos de seguridad

Existen varias metodologías que pueden ayudar en la clasificación de riesgos que tienen los entornos virtualizados. Dependiendo de cada una, se pueden encontrar soluciones a la seguridad a la arquitectura en referencia y controles que se pueden aplicar. En la tabla 7, se muestran varias opciones:

Tabla 7:
Metodologías en evaluación de riesgos

DESCRIPCIÓN	ZERO TRUST	MAGERIT	OCTAVE
Evaluación	✓	✓	✓
Identificación de activos	✓	✓	✓
Valoración de activos	✓	✓	✓
Impedir	✓	X	X
Diseño de la seguridad para reducir el riesgo. (frecuencia, Degradación, Impacto, cálculo del riesgo)	✓	✓	✓
Seguridad automatizada para reducir la complejidad y evitar errores humanos.	✓	X	X
Seguridad continua y siempre activa para una protección efectiva	✓	X	X

Nota*:* Autoría propia, basado en características de los modelos Zero Trust, Magerit y Octave

CAPÍTULO II: ARTÍCULO PROFESIONAL

2.1 Resumen

Los entornos virtuales son muy importantes en la actualidad porque nos permite tener varios recursos virtualizados con una mínima inversión de infraestructura, garantizando el funcionamiento de una organización debido a que se puede virtualizar bases de datos, sistemas operativos, aplicaciones, etc., el control de toda la virtualización se la realiza con la ayuda de hipervisores que permite tener el control de todo el entorno virtual, por lo que son muy susceptibles a ataques cibernéticos. Estás amenazas o vulnerabilidades pueden tener repercusiones para la empresa que tiene implementada estos entornos, por esta razón plantea una guía para seleccionar la metodología acorde a los requisitos de cada empresa.

Palabras clave: hipervisores, entornos, metodología, virtualidad, seguridad.

2.2 Abstract

Virtual environments are very important today because it allows us to have several virtualized resources with a minimum investment in infrastructure, guaranteeing the operation of an organization because it is possible to virtualize databases, operating systems, applications, etc., the control of All virtualization is done with the help of hypervisors that allow control of the entire virtual environment, which is why they are very susceptible to cyber attacks. These threats or vulnerabilities can have repercussions for the company that has implemented these environments, for this reason it proposes a guide to select the methodology according to the requirements of each company.

Keywords: hypervisors, environments, methodology, virtuality, security.

2.3 Introducción

El avance tecnológico de los últimos años ha crecido de una manera significativa por tal motivo gran parte de las empresas se vieron en la necesidad de acoplarse a este avance tecnológico, por tal motivo han evolucionado sus infraestructuras para poder soportar los servicios que brindan.

Según IONOS Digital Guide. (2019), la virtualización de los sistemas es primordial para el desarrollo de infraestructuras dentro de las organizaciones. En estos entornos las partes interesadas, clientes y proveedores; cuestiona la seguridad en varios niveles y como consecuencia la seguridad de la virtualización de los sistemas subyacentes, como son los niveles de servicios (SLA), acceso a los recursos y la restricción de acceso a datos no autorizados, para garantizar la confidencialidad e integridad de los recursos.

La virtualización ha realizado esfuerzos para mejorar el rendimiento con la aparición de nuevas tecnologías, y hace referencia para la creación de máquinas virtuales a través de la virtualización del hardware, software, almacenamiento, red y datos.

La implementación de estos modelos de virtualización podrían verse afectada por ataques de ciberdelincuentes y provocar el aislamiento de los hipervisores, los mismos que se intercomunican entre las capas verticales de su estructura y sería extremadamente difícil de establecer una seguridad de defensa profunda.

2.4 Metodología

Para el desarrollo del trabajo se ha utilizado un proceso de investigación cualitativa exploratorio con la revisión de artículos de investigación, tesis, determinando como los métodos de seguridad de tecnología servirá de guía y permita elegir una estrategia para la protección en los hipervisores.

Análisis de amenazas y ataques

«Utilizando las metodologías de modelos de seguridad para analizar las amenazas y ataques que se relacionan con la arquitectura de referencia, se considera un conjunto principal de amenazas, suplantación de identidad, manipulación, repudio, divulgación de información, denegación de servicio y elevación de privilegios.» (Shashank Guptah, 2017).

En la tabla 8, se evidencia que el objetivo de estos ataques, principalmente son máquinas virtuales e hipervisores.

Tabla 8:

Relación de amenazas y ataques a la arquitectura en referencia

		Suplantación de identidad	Manipulación	Repudio	Divulgación de información	Negación de servicio	Elevación de privilegio
Hipervisor TIPO 1	Máquina Virtual	Hyperjacking VM movilidad	Diseño Software defectuoso Exploits en software de aplicación VM Hopping VM Escape VM	Supervisión entre máquinas virtuales Supervisión de máquina virtuales y el host	Exploits en software de aplicación Supervisión entre máquinas virtuales Supervisión de máquina virtuales y el host	Denegación de servicios entre máquinas virtuales	Exploits en software de aplicación VM Hopping VM Escape VM

		Suplantación de identidad	Manipulación	Repudio	Divulgación de información	Negación de servicio	Elevación de privilegio
Hipervisor TIPO 1	Hypervisor		Explotación al canal de control Explotación al hipervisor Escape de la máquina virtual y el host	Explotación al canal de control Explotación al hipervisor	Explotación al hipervisor Cálculo de monopolización	Denegación de servicios al hipervisor	VM Escape VM
Hipervisor TIPO 2	Sistema Operativo		VM Escapto VM			Denegación de servicios de hipervisor	VM Escape VM
Hipervisor TIPO 1	Hardware		Explotación al Firmware		Explotación al Firmware	Denegación de servicios al hipervisor	Explotación al Firmware

Fuente: Por el autor, basado en artículo Shashank Guptah, 2017

Los elementos críticos analizados servirán como guía al personal de seguridad en qué elementos deben tener mayor cuidado dentro de los entornos virtualizados.

- Las aplicaciones de máquinas virtuales, crean instancias que exponen interfaces que se pueden acceder de forma remota, el atacante externo de forma remota puede usar las interfaces expuestas.
- La capa de hardware no es accesible para el atacante de forma remota, por lo que se considera una intrusión física fuera de la virtualización.
- Los activos a los que se dirige el atacante son aplicaciones y datos ubicados en máquinas virtuales.
- El objetivo de los atacantes es impactar de forma negativa en la disponibilidad de servicio, la integridad (alteración) o la confidencialidad (recuperación) de un activo.
- Los componentes se consideran seguros si no están comprometidos, pero los mismos pueden contener fallas en el software inherentes que pueden ser conocidas por el atacante, el atacante las puede explotar para comprometer algún componente y obtener influencia o control sobre él.

Mecanismos de seguridad

Las contramedidas consisten en la protección de recursos o componentes y estos deben ser considerados al momento de diseñar e integrar los mecanismos de seguridad, estas contramedidas puede afectar tanto a las máquinas virtuales como al hipervisor.

Según Compastié (2020), la protección de recursos de la máquina virtual y hipervisores se los realiza en la integración de mecanismos de seguridad al momento de diseño de la máquina virtual y hipervisor.

Máquina Virtual

- Kernel del sistema operativo.
- Basado en Aplicaciones.
- Gestión de software seguro.

Hipervisor

- Entorno de ejecución
- Granularidad del hipervisor
- protección de Redes y Almacenamiento

Se detalla en la tabla 9 se detalla las contramedidas al momento de integración de mecanismos de seguridad en tiempo de diseño. A las máquinas virtuales y hipervisores

Tabla 9:
Contramedidas al momento de integración.

Mecanismo	Área de Protección	Contramedidas	Cobertura	Requisitos
Integración de Mecanismos de Seguridad en Tiempo de Diseño	Protección Máquina Virtual	Contador basado en la medida de kernel	kernel del sistema operativo, Kernel del sistema operativo host	Existencia de implementaciones de mecanismos para los núcleos operados
		Basado en aplicaciones	Solicitud, tiempo de ejecución	Existencia de implementaciones de mecanismos para todas las aplicaciones operadas y su tiempo de ejecución
		Gestión de software seguro	kernel del sistema operativo, Aplicación, tiempo de ejecución	Gestión de software seguro solo para los administradores de paquetes
	Protección Hipervisor	Entorno de ejecución	Hipervisor, Kernel del sistema operativo host	implementación de mecanismos en los hipervisores operados
		Granularidad del hipervisor	hipervisor	Arquitectura modular del hipervisor
		Protección de Redes y Almacenamiento	hipervisor	Dispositivos de almacenamiento y redes. Interfaces del hipervisor

Nota: Por el autor, basado en el artículo Compastié 2020

Para minimizar la superficie de ataque se debe enfocar en las técnicas de verificación y caídas de capacidades del recurso, esto nos permite evaluar las propiedades de seguridad

en los componentes de la arquitectura y también verificar el diseño de los mecanismos de seguridad:

- Verificación formal de Código
- Reducción de procesos innecesarios en el Procesador
- Externalización de VM Gestión de software

Se detalla en la tabla 10 se detalla las contramedidas para minimizar la superficie de ataque:

Tabla 10:
Contramedidas para minimizar superficie de ataque.

Mecanismo	Contramedidas	Cobertura	Requisitos
Minimización de la superficie de ataque	Verificación formal de Código	Núcleo del sistema operativo, hipervisor, Kernel del sistema operativo host	Base de código, diseño y mantenibilidad limitados al momento de la ejecución de pruebas
	Reducción de procesos innecesarios en el Procesador	Todos los componentes de software	Diseño modular y soporte para deshabilitar características en tiempo de ejecución
	Externalización de VM Gestión de software	Aplicación, tiempo de ejecución, núcleo del sistema operativo	Instancia de máquina virtual de corta duración, imagen protegida en el entorno de construcción

Nota: Por el autor, basado en el artículo Compastié 2020

La adaptación basada en la programabilidad de seguridad como contramedida son eficientes en la reducción de la superficie de ataque, pero deben irse adaptando constantemente en el tiempo para enfrentarse a nuevas amenazas y ataques. La programabilidad de recursos y mecanismos de seguridad puede ser impulsado por una actividad que se base en los resultados de la supervisión.

Se detalla en la tabla 11 las contramedidas para la adaptación basada en la programabilidad de seguridad.

Tabla 11:
Contramedidas para programabilidad de seguridad.

Mecanismo	Contramedidas	Cobertura	Requisitos
Adaptación basada en Seguridad Programabilidad	Seguimiento de recursos compartidos	Aplicación, tiempo de ejecución, núcleo del sistema operativo	Existencia de interfaces para monitorear y conocimiento necesario para el monitore de datos
	Controles de Seguridad a los Mecanismos	Aplicación, tiempo de ejecución, núcleo del sistema operativo	Especificación de los requisitos de seguridad y características del mecanismo
	Programabilidad de seguridad	Aplicación, tiempo de ejecución, núcleo del sistema operativo	Interfaces de reconfiguración, o posibilidad de reiniciar componentes

Nota: Por el autor, basado en el artículo Compastié 2020

2.5 Resultados y Discusión

Resultados

Se plantea la utilización del modelo *Zero Trust* como estrategia para minimizar las vulnerabilidades que afectan a los hipervisores.

Primer Paso: Recopilación de información

Lo primero en esta etapa es recopilar toda la información de empleados, dispositivos que se conectan a los diferentes aplicativos que disponga la empresa y validar que los privilegios de acceso disponen.

Segundo paso: Detección de factores de riesgo

Evaluar las condiciones óptimas y adversas que rodean a la empresa, para preparar de una forma adecuada de tal modo que esas debilidades y amenazas tengan un menor impacto e impida el correcto funcionamiento de esta.

Los componentes para evaluar serían:

- Personas: Son el eslabón más débil en las prácticas de seguridad, por lo que se deben alinear con la estrategia de controles y limitaciones de accesos con los privilegios mínimos.
- Operaciones: las protecciones de carga de trabajo es una responsabilidad compartida entre el cliente y el proveedor de servicios, se debe establecer un proceso y estructura de gobernanza, realizar un inventario y supervisión de las configuraciones y centrarse en soluciones de seguridad en la nube.

- Dispositivos: se deben establecer segmentos pequeños a los que pueden conectarse los dispositivos sin tener acceso a la totalidad de la red, mantener actualizados los dispositivos IOT para los componentes de seguridad y crear políticas de seguridad sobre los dispositivos BYOD.
- Redes: Se debe crear límites mediante la segmentación lógica alrededor de los activos de la red y aumentar el aislamiento entre segmentos.
- Datos: Se debe clasificar cuáles son los datos confidenciales y el lugar donde se encuentran para proteger esta información.

Tercer Paso: Seguridad de la red

La capa de seguridad de red implementa políticas y controles para permitir a los usuarios tener acceso autorizados a los recursos de red.

- Control de acceso: Se debe controlar a los usuarios qué tipo de acceso y secciones puede acceder de acuerdo con su nivel de privilegios.
- Segmentación de la red: Se debe dividir la red en segmentos lógicos pequeños para poder añadir controles entre segmentos y mejorar el rendimiento y la seguridad. La segmentación de red permitirá la asignación o denegación de credenciales de autorización para empleados y garantizar que nadie acceda a información no autorizada.
- Cifrado: se debe clasificar el tipo de cifrado de acuerdo con el método que se va a utilizar, los mismos que pueden ser cifrado de bloques, algoritmos de clave simétrica/asimétrica o algoritmos de hash.

Discusión

Con las metodologías de gestión de riesgo se pueden identificar cada uno de los activos y las amenazas a las que están expuestos los hipervisores y generar una guía que se acople a las empresas al grado de seguridad que deseen incorporar.

CONCLUSIONES

- Se estudiaron las características de los modelos existentes para el análisis de protección de datos y entender el contexto del paradigma de la seguridad en la información, observando a los métodos tradicionales asumir que todos los elementos que se encuentran dentro de la red en las empresas son confiables. La tendencia a nuevas modalidades de trabajos y ataques de vulnerabilidades que se encuentran en los sistemas.

- El presente documento analizó las vulnerabilidades para la protección de los hipervisores, las mismas que pueden originarse por intrusos internos con la intención maliciosa y causar daños por parte de un atacante desde el exterior de la red. Se expuso los factores que pueden provocar estas vulnerabilidades como el descontento de empleados y que puedan interferir en el correcto funcionamiento de los sistemas generando un impacto en la estructura de negocio de la empresa.
- En la categorización de los riesgos se tomó como base al Sistema de Gestión de Seguridad de la Información (SGSI), para establecer criterios y niveles de riesgo que afecten las credenciales, integridad y disponibilidad de los sistemas
- Se realizó una comparativa de la metodología de seguridad de riesgos y que se pueden acoger de acuerdo con las necesidades de la empresa.

RECOMENDACIONES

- Para la implantación de la metodología de seguridad primero se debe cambiar la mentalidad de los profesionales de la seguridad, el proceso en la implementación es lento y paulatino ya que se debe socializar los conceptos de la metodología dentro de toda la organización.
- En el mercado existe gran variedad de equipos como computadores y móviles los mismos permiten la comunicación y conexión entre clientes, proveedores y empleados a los sistemas de la empresa. Esto genera una gran cantidad de requisitos y protocolos de comunicación que deben ser controlados y rastreados de forma continua, esta relación de protocolos y equipos debe ir de la mano con la investigación de nuevas soluciones para futuras investigaciones.
- Las empresas en la actualidad deben buscar modelos de seguridad capaces de adaptarse de forma rápida y eficaz a los entornos modernos, que permita proteger a las personas, dispositivos, datos y aplicaciones en cualquier parte que se encuentren.
- Para la implementación de un modelo en las empresas se debe cumplir con todos los requisitos indicados en los modelos para que puedan ir acoplándose con las tecnologías existentes y brindando la seguridad en cada una de las etapas de implantación, el factor humano es fundamental para el cumplimiento de cada proceso.
- Es recomendable que las personas que están enfrentando los desafíos de la seguridad a nivel de máquinas virtuales y de sus hipervisores, conozcan realmente el funcionamiento de la tecnología, para que puedan aportar con el manejo de la seguridad.

Bibliografía

Arévalo Cordovilla, F., Arévalo Cordovilla, B., Castillo Salvatierra, L., & Cortez Lara, A. (2021). *Gestión de Seguridad en Virtualización de Servidores. Ecuadorian Science Journal, 5(4), 150–163.* https://doi.org/10.46480/esj.5.4.178

Bhagat, S. P., Patil, V. S., & Meshram, B. B. (2020). *Security issues due to vulnerabilities in the virtual machine of cloud computing.* En Intelligent Computing and Communication (pp. 625–634). Springer Singapore.

Castillo, J. A. (2018). *Qué es la virtualización y para qué sirve. Profesional Review.* https://www.profesionalreview.com/2018/11/05/que-es-virtualizacion/

Compastié, M., Badonnel, R., Festor, O., & He, R. (2020). *From virtualization security issues to cloud protection opportunities: An in-depth analysis of system virtualization models. Computers & Security, 97(101905), 101905*. https://doi.org/10.1016/j.cose.2020.101905

de la Cruz, H. (2021). *Metodología OCTAVE para el análisis de riesgos en SGSI. PMG SSI - ISO 27001.* https://www.pmg-ssi.com/2021/09/metodologia-octave-para-el-analisis-de-riesgos-en-sgsi/

IBM Cloud Education. (2019). *Ibm.com.* https://www.ibm.com/mx-es/cloud/learn/hypervisors

IONOS Digital Guide. (2019). *Virtualización: el alma de la nube*, de https://www.ionos.es/digitalguide/servidores/configuracion/virtualizacion/

Limones, E. (2021). *Virtualización: Tipos y software utilizado. OpenWebinars.net.* https://openwebinars.net/blog/virtualizacion-tipos-y-software-utilizado/

MAGERIT v.3 :(2020) *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. (n.d.). Gob.es. Retrieved August 13, 2022*, from https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Shashank Guptah (2017). *Detection Avoidance and Attack Pattern Mechanisms in Modern Web Application Vulnerabilities* https://www.researchgate.net/publication/317014729_Detection_Avoidance_and_Attack_Pattern_Mechanisms_in_Modern_Web_Application_Vulnerabilities_Present_and_Future_Challenges

Vmware (2020). *Cvedetails.com. Retrieved August 14, 2022,* from https://www.cvedetails.com/vulnerability-list/vendor_id-252/product_id-22134/version_id-633765/Vmware-Esxi-6.5.html

Zero trust maturity model. (2020.). *Cisa.gov.* https://www.cisa.gov/zero-trust-maturity-model

ANEXO

ANEXO 1

Common Vulnerabilities and Exposures hasta febrero de 2023

ANEXO 2

Relación de amenazas y ataques por componentes

ANEXO 3

Configuración de contramedidas para minimizar ataques

Anexo 1

Tabla 1

Common Vulnerabilities and Exposures tomados desde 2021 hasta febrero de 2023

CVE	Descripción
CVE-2022-35867	Esta vulnerabilidad permite a los atacantes locales aumentar los privilegios en las instalaciones afectadas de xhyve. Un atacante primero debe obtener la capacidad de ejecutar código con privilegios elevados en el sistema invitado de destino para aprovechar esta vulnerabilidad. La falla específica existe dentro del dispositivo virtual e1000. El problema se debe a la falta de una validación adecuada de la longitud de los datos proporcionados por el usuario antes de copiarlos en un búfer basado en pila. Un atacante puede aprovechar esta vulnerabilidad para aumentar los privilegios y ejecutar código arbitrario en el contexto del hipervisor. Era ZDI-CAN-15056.
CVE-2022-34889	Esta vulnerabilidad permite a los atacantes locales aumentar los privilegios en las instalaciones afectadas de Parallels Desktop 17.1.1 (51537). Un atacante primero debe obtener la capacidad de ejecutar código con privilegios elevados en el sistema invitado de destino para aprovechar esta vulnerabilidad. La falla específica existe dentro del dispositivo virtual ACPI. El problema se debe a la falta de una validación adecuada de los datos proporcionados por el usuario, lo que puede resultar en una lectura más allá del final de un búfer asignado. Un atacante puede aprovechar esta vulnerabilidad para aumentar los privilegios y ejecutar código arbitrario en el contexto del hipervisor. Era ZDI-CAN-16554.
CVE-2022-32295	En los dispositivos Ampere Altra y AltraMax anteriores a SRP 1.09, el diseño de referencia de Altra de los accesos UEFI permite el acceso inseguro a SPI-NOR por parte del componente OS/hipervisor.
CVE-2022-25681	Posible corrupción de la memoria en el kernel al realizar el acceso a la memoria debido a que el hipervisor no invalidó correctamente las cachés de traducción del procesador en Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile
CVE-2022-23034	Un invitado de PV podría DoS Xen mientras desasigna una concesión Para abordar XSA-380, se introdujo el recuento de referencias para las asignaciones de concesión en el caso de que un invitado de PV tuviera IOMMU habilitado. Los huéspedes de PV pueden solicitar dos formas de asignaciones. Cuando ambos están en uso para cualquier asignación individual, se puede solicitar la eliminación de dicha asignación en dos pasos. El recuento de referencia para tal mapeo se reduciría dos veces por error. Se detecta el subdesbordamiento de los contadores, lo que provoca la activación de una comprobación de errores del hipervisor.
CVE-2022-23030	En la versión 16.1.x anterior a la 16.1.2, 15.1.x anterior a la 15.1.4.1, 14.1.x anterior a la 14.1.4.5 y todas las versiones de 13.1.x, cuando BIG-IP Virtual Edition (VE) usa el controlador ixlv (que se usa en modo SR-IOV y requiere la familia de adaptadores de red Intel X710/XL710/XXV710 en el hipervisor) y la configuración de descarga de segmentación TCP está habilitada, las solicitudes no reveladas pueden causar un aumento en la utilización de recursos de la CPU. Nota: No se evalúan las versiones de software que han llegado al final del soporte técnico (EoTS).
CVE-2022-22093	Corrupción de la memoria o denegación temporal del servicio debido al manejo inadecuado de operaciones simultáneas de hipervisor para adjuntar o desconectar IRQ de fuentes de interrupción virtual en Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile
CVE-2022-21816	El software NVIDIA vGPU contiene una vulnerabilidad en Virtual GPU Manager (nvidia.ko), donde un usuario en el sistema operativo invitado puede provocar una tormenta de interrupción de GPU en el host del hipervisor, lo que lleva a una denegación de servicio.
CVE-2021-46744	Un atacante con acceso a un hipervisor malicioso puede inferir valores de datos utilizados en un huésped SEV en CPU AMD al monitorear los valores de texto cifrado a lo largo del tiempo.
CVE-2021-38937	IBM PowerVM Hypervisor FW940, FW950 y FW1010 podrían permitir que un usuario autenticado provoque que el sistema se bloquee mediante una llamada de IBMi Hypervisor especialmente diseñada. Identificación de IBM X-Force: 210894.
CVE-2021-38923	IBM PowerVM Hypervisor FW1010 podría permitir que un usuario privilegiado obtenga acceso a otra VM debido a la asignación de WWPN duplicados. Identificación de IBM X-Force: 210162.
CVE-2021-38918	IBM PowerVM Hypervisor FW860, FW940, FW950 y FW1010, a través de una secuencia específica de operaciones de administración de VM, podría provocar una violación del aislamiento entre las VM del mismo nivel. Identificación de IBM X-Force: 210019.

CVE	Descripción
CVE-2021-38917	IBM PowerVM Hypervisor FW860, FW940 y FW950 podría permitir que un atacante que obtenga acceso de servicio al FSP pueda leer y escribir en la memoria del sistema host arbitrario a través de una serie de procedimientos de servicio cuidadosamente diseñados. Identificación de IBM X-Force: 210018.
CVE-2021-36148	Se descubrió un problema en ACRN antes de 2.5. dmar_free_irte en hypervisor/arch/x86/vtd.c permite un desbordamiento de búfer irte_alloc_bitmap.
CVE-2021-35101	El manejo inadecuado de las escrituras en el control GICR virtual puede provocar una falla de aserción en el hipervisor en Snapdragon Auto, Snapdragon Compute, Snapdragon Mobile
CVE-2021-35090	Posible corrupción de la memoria del hipervisor debido a la condición de carrera TOC TOU al actualizar las asignaciones de direcciones en Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile
CVE-2021-34987	Esta vulnerabilidad permite a los atacantes locales aumentar los privilegios en las instalaciones afectadas de Parallels Desktop 16.5.1 (49187). Un atacante primero debe obtener la capacidad de ejecutar código con privilegios elevados en el sistema invitado de destino para aprovechar esta vulnerabilidad. La falla específica existe dentro del dispositivo virtual HDAudio. El problema se debe a la falta de una validación adecuada de la longitud de los datos proporcionados por el usuario antes de copiarlos en un búfer de longitud fija. Un atacante puede aprovechar esta vulnerabilidad para aumentar los privilegios y ejecutar código arbitrario en el contexto del hipervisor. Era ZDI-CAN-14969.
CVE-2021-34869	Esta vulnerabilidad permite a los atacantes locales aumentar los privilegios en las instalaciones afectadas de Parallels Desktop 16.1.3-49160. Un atacante primero debe obtener la capacidad de ejecutar código con pocos privilegios en el sistema huésped de destino para aprovechar esta vulnerabilidad. La falla específica existe dentro del componente Toolgate. El problema se debe a la falta de una validación adecuada de los datos proporcionados por el usuario, lo que puede provocar una asignación de memoria descontrolada. Un atacante puede aprovechar esta vulnerabilidad para aumentar los privilegios y ejecutar código arbitrario en el contexto del hipervisor. Era ZDI-CAN-13797.
CVE-2021-34868	Esta vulnerabilidad permite a los atacantes locales aumentar los privilegios en las instalaciones afectadas de Parallels Desktop 16.1.3-49160. Un atacante primero debe obtener la capacidad de ejecutar código con pocos privilegios en el sistema huésped de destino para aprovechar esta vulnerabilidad. La falla específica existe dentro del componente Toolgate. El problema se debe a la falta de una validación adecuada de los datos proporcionados por el usuario, lo que puede provocar una asignación de memoria descontrolada. Un atacante puede aprovechar esta vulnerabilidad para aumentar los privilegios y ejecutar código arbitrario en el contexto del hipervisor. Era ZDI-CAN-13712.
CVE-2021-34867	Esta vulnerabilidad permite a los atacantes locales aumentar los privilegios en las instalaciones afectadas de Parallels Desktop 16.1.3-49160. Un atacante primero debe obtener la capacidad de ejecutar código con privilegios elevados en el sistema invitado de destino para aprovechar esta vulnerabilidad. La falla específica existe dentro del componente Toolgate. El problema se debe a la falta de una validación adecuada de los datos proporcionados por el usuario, lo que puede provocar una asignación de memoria descontrolada. Un atacante puede aprovechar esta vulnerabilidad para aumentar los privilegios y ejecutar código arbitrario en el contexto del hipervisor. Era ZDI-CAN-13672.
CVE-2021-34864	Esta vulnerabilidad permite a los atacantes locales aumentar los privilegios en las instalaciones afectadas de Parallels Desktop 16.1.3 (49160). Un atacante primero debe obtener la capacidad de ejecutar código con pocos privilegios en el sistema huésped de destino para aprovechar esta vulnerabilidad. La falla específica existe dentro del componente WinAppHelper. El problema se debe a la falta de un control de acceso adecuado. Un atacante puede aprovechar esta vulnerabilidad para aumentar los privilegios y ejecutar código arbitrario en el contexto del hipervisor. Era ZDI-CAN-13543.
CVE-2021-34857	Esta vulnerabilidad permite a los atacantes locales aumentar los privilegios en las instalaciones afectadas de Parallels Desktop 16.1.3 (49160). Un atacante primero debe obtener la capacidad de ejecutar código con privilegios elevados en el sistema invitado de destino para aprovechar esta vulnerabilidad. La falla específica existe dentro del componente Toolgate. El problema se debe a la falta de una validación adecuada de los datos proporcionados por el usuario, lo que puede resultar en una escritura más allá del final de un búfer asignado. Un atacante puede aprovechar esta vulnerabilidad para aumentar los privilegios y ejecutar código arbitrario en el contexto del hipervisor. Era ZDI-CAN-13601.
CVE-2021-34856	Esta vulnerabilidad permite a los atacantes locales aumentar los privilegios en las instalaciones afectadas de Parallels Desktop 16.1.3 (49160). Un atacante primero debe obtener la capacidad de ejecutar código con privilegios elevados en el sistema invitado de destino para aprovechar esta vulnerabilidad. La falla específica existe dentro del dispositivo

CVE	Descripción
	virtual virtio-gpu. El problema se debe a la falta de una validación adecuada de los datos proporcionados por el usuario, lo que puede provocar una condición de corrupción de la memoria. Un atacante puede aprovechar esta vulnerabilidad para aumentar los privilegios y ejecutar código arbitrario en el contexto del hipervisor. Era ZDI-CAN-13581.
CVE-2021-34855	Esta vulnerabilidad permite a los atacantes locales revelar información confidencial sobre las instalaciones afectadas de Parallels Desktop 16.1.3 (49160). Un atacante primero debe obtener la capacidad de ejecutar código con pocos privilegios en el sistema huésped de destino para aprovechar esta vulnerabilidad. La falla específica existe dentro del componente Toolgate. El problema se debe a la falta de inicialización adecuada de la memoria antes de acceder a ella. Un atacante puede aprovechar esto junto con otras vulnerabilidades para aumentar los privilegios y ejecutar código arbitrario en el contexto del hipervisor. Era ZDI-CAN-13592.
CVE-2021-34854	Esta vulnerabilidad permite a los atacantes locales aumentar los privilegios en las instalaciones afectadas de Parallels Desktop 16.1.3 (49160). Un atacante primero debe obtener la capacidad de ejecutar código con pocos privilegios en el sistema huésped de destino para aprovechar esta vulnerabilidad. La falla específica existe dentro del componente Toolgate. El problema se debe a la falta de una validación adecuada de los datos proporcionados por el usuario, lo que puede provocar una asignación de memoria descontrolada. Un atacante puede aprovechar esta vulnerabilidad para aumentar los privilegios y ejecutar código arbitrario en el contexto del hipervisor. Era ZDI-CAN-13544.
CVE-2021-32847	HyperKit es un conjunto de herramientas para incorporar capacidades de hipervisor en una aplicación. En las versiones 0.20210107 y anteriores, un huésped malicioso puede desencadenar una vulnerabilidad en el host al abusar del controlador de disco que puede provocar la divulgación de la memoria del host en el huésped virtualizado. Este problema se corrige en la confirmación cf60095a4d8c3cb2e182a14415467afd356e982f.
CVE-2021-32846	HyperKit es un conjunto de herramientas para incorporar capacidades de hipervisor en una aplicación. En las versiones 0.20210107, la función `pci_vtsock_proc_tx` en `virtio-sock` puede conducir al uso de memoria no inicializada. En esta situación, hay una verificación para que el valor de retorno sea menor o igual a `VTSOCK_MAXSEGS`, pero esa verificación no es suficiente porque la función puede devolver `-1` si encuentra un error del que no puede recuperarse. Además, `iovec_pull` usará el valor de retorno negativo en una condición while que puede conducir a más corrupción porque la función no está diseñada para manejar un `iov_len` negativo. Este problema puede provocar que un invitado bloquee el host, lo que provoca una denegación de servicio y, en determinadas circunstancias, daños en la memoria. Este problema se corrige en la confirmación af5eba2360a7351c08dfd9767d9be863a50ebaba.
CVE-2021-32845	HyperKit es un conjunto de herramientas para incorporar capacidades de hipervisor en una aplicación. En las versiones 0.20210107 y anteriores de HyperKit, la implementación de `qnotify` en `pci_vtrnd_notify` no comprueba el valor de retorno de `vq_getchain`. Esto lleva a que `struct iovec iov;` no se inicialice y se use para leer la memoria en `len = (int) read(sc->vrsc_fd, iov.iov_base, iov.iov_len);` cuando un atacante puede hacer `vq_getchain` fallar. Este problema puede provocar que un invitado bloquee el host, lo que provoca una denegación de servicio y, en determinadas circunstancias, daños en la memoria. Este problema se solucionó en la confirmación 41272a980197917df8e58ff90642d14dec8fe948.
CVE-2021-32844	HyperKit es un conjunto de herramientas para incorporar capacidades de hipervisor en una aplicación. En las versiones 0.20210107 y anteriores de HyperKit, `vi_pci_write` tiene una llamada a `vc_cfgwrite` que no busca valores nulos, lo que hace que el host se bloquee cuando se llama. Este problema puede provocar que un invitado bloquee el host y provoque una denegación de servicio. Este problema se solucionó en la confirmación 451558fe8aaa8b24e02e34106e3bb9fe41d7ad13.
CVE-2021-32843	HyperKit es un conjunto de herramientas para incorporar capacidades de hipervisor en una aplicación. En las versiones 0.20210107 y anteriores de HyperKit, `virtio.c` tiene una llamada a `vc_cfgread` que no busca valores nulos que, cuando se llama, hace que el host se bloquee. Este problema puede provocar que un invitado bloquee el host y provoque una denegación de servicio. Este problema se solucionó en la confirmación df0e46c7dbfd81a957d85e449ba41b52f6f7beb4.
CVE-2021-31432	Esta vulnerabilidad permite a los atacantes locales revelar información confidencial sobre las instalaciones afectadas de Parallels Desktop 15.1.5-47309. Un atacante primero debe obtener la capacidad de ejecutar código con privilegios elevados en el sistema invitado de destino para aprovechar esta vulnerabilidad. La falla específica existe dentro del dispositivo virtual IDE. El problema se debe a la falta de una validación adecuada de los datos proporcionados por el usuario, lo que puede resultar en una lectura más allá del final de un búfer asignado. Un atacante puede aprovechar esto junto con otras vulnerabilidades para

CVE	Descripción
	aumentar los privilegios y ejecutar código arbitrario en el contexto del hipervisor. Era ZDI-CAN-13190.
CVE-2021-31431	Esta vulnerabilidad permite a los atacantes locales revelar información confidencial sobre las instalaciones afectadas de Parallels Desktop 15.1.5-47309. Un atacante primero debe obtener la capacidad de ejecutar código con privilegios elevados en el sistema invitado de destino para aprovechar esta vulnerabilidad. La falla específica existe dentro del dispositivo virtual IDE. El problema se debe a la falta de una validación adecuada de los datos proporcionados por el usuario, lo que puede resultar en una lectura más allá del final de un búfer asignado. Un atacante puede aprovechar esto junto con otras vulnerabilidades para aumentar los privilegios y ejecutar código arbitrario en el contexto del hipervisor. Era ZDI-CAN-13189.
CVE-2021-31430	Esta vulnerabilidad permite a los atacantes locales revelar información confidencial sobre las instalaciones afectadas de Parallels Desktop 15.1.5-47309. Un atacante primero debe obtener la capacidad de ejecutar código con privilegios elevados en el sistema invitado de destino para aprovechar esta vulnerabilidad. La falla específica existe dentro del dispositivo virtual IDE. El problema se debe a la falta de una validación adecuada de los datos proporcionados por el usuario, lo que puede resultar en una lectura más allá del final de un búfer asignado. Un atacante puede aprovechar esto junto con otras vulnerabilidades para aumentar los privilegios y ejecutar código arbitrario en el contexto del hipervisor. Era ZDI-CAN-13188.
CVE-2021-31429	Esta vulnerabilidad permite a los atacantes locales aumentar los privilegios en las instalaciones afectadas de Parallels Desktop 15.1.5-47309. Un atacante primero debe obtener la capacidad de ejecutar código con privilegios elevados en el sistema invitado de destino para aprovechar esta vulnerabilidad. La falla específica existe dentro del dispositivo virtual IDE. El problema se debe a la falta de una validación adecuada de la longitud de los datos proporcionados por el usuario antes de copiarlos en un búfer basado en almacenamiento dinámico de longitud fija. Un atacante puede aprovechar esta vulnerabilidad para aumentar los privilegios y ejecutar código arbitrario en el contexto del hipervisor. Era ZDI-CAN-13187.
CVE-2021-31428	Esta vulnerabilidad permite a los atacantes locales aumentar los privilegios en las instalaciones afectadas de Parallels Desktop 15.1.5-47309. Un atacante primero debe obtener la capacidad de ejecutar código con privilegios elevados en el sistema invitado de destino para aprovechar esta vulnerabilidad. La falla específica existe dentro del dispositivo virtual IDE. El problema se debe a la falta de una validación adecuada de la longitud de los datos proporcionados por el usuario antes de copiarlos en un búfer basado en almacenamiento dinámico de longitud fija. Un atacante puede aprovechar esta vulnerabilidad para aumentar los privilegios y ejecutar código arbitrario en el contexto del hipervisor. Era ZDI-CAN-13186.
CVE-2021-31427	Esta vulnerabilidad permite a los atacantes locales revelar información confidencial sobre las instalaciones afectadas de Parallels Desktop 15.1.5-47309. Un atacante primero debe obtener la capacidad de ejecutar código con pocos privilegios en el sistema huésped de destino para aprovechar esta vulnerabilidad. La falla específica existe dentro del componente Open Tools Gate. El problema se debe a la falta de bloqueo adecuado al realizar operaciones en un objeto. Un atacante puede aprovechar esto junto con otras vulnerabilidades para aumentar los privilegios y ejecutar código arbitrario en el contexto del hipervisor. Era ZDI-CAN-13082.
CVE-2021-31424	Esta vulnerabilidad permite a los atacantes locales aumentar los privilegios en las instalaciones afectadas de Parallels Desktop 15.1.5-47309. Un atacante primero debe obtener la capacidad de ejecutar código con pocos privilegios en el sistema huésped de destino para aprovechar esta vulnerabilidad. La falla específica existe dentro del componente Open Tools Gate. El problema se debe a la falta de una validación adecuada de la longitud de los datos proporcionados por el usuario antes de copiarlos en un búfer basado en almacenamiento dinámico de longitud fija. Un atacante puede aprovechar esta vulnerabilidad para aumentar los privilegios y ejecutar código arbitrario en el contexto del hipervisor. Era ZDI-CAN-12848.
CVE-2021-31423	Esta vulnerabilidad permite a los atacantes locales revelar información confidencial sobre las instalaciones afectadas de Parallels Desktop 15.1.5-47309. Un atacante primero debe obtener la capacidad de ejecutar código con privilegios elevados en el sistema invitado de destino para aprovechar esta vulnerabilidad. La falla específica existe dentro del componente Toolgate. El problema se debe a la falta de inicialización adecuada de la memoria antes de acceder a ella. Un atacante puede aprovechar esto junto con otras

CVE	Descripción
	vulnerabilidades para aumentar los privilegios y ejecutar código arbitrario en el contexto del hipervisor. Era ZDI-CAN-12528.
CVE-2021-31422	Esta vulnerabilidad permite a los atacantes locales aumentar los privilegios en las instalaciones afectadas de Parallels Desktop 16.1.1-49141. Un atacante primero debe obtener la capacidad de ejecutar código con privilegios elevados en el sistema invitado de destino para aprovechar esta vulnerabilidad. La falla específica existe dentro del dispositivo virtual e1000e. El problema se debe a la falta de bloqueo adecuado al realizar operaciones en un objeto. Un atacante puede aprovechar esta vulnerabilidad para aumentar los privilegios y ejecutar código arbitrario en el contexto del hipervisor. Era ZDI-CAN-12527.
CVE-2021-31421	Esta vulnerabilidad permite a atacantes locales eliminar archivos arbitrarios en instalaciones afectadas de Parallels Desktop 16.1.1-49141. Un atacante primero debe obtener la capacidad de ejecutar código con privilegios elevados en el sistema invitado de destino para aprovechar esta vulnerabilidad. La falla específica existe dentro del componente Toolgate. El problema se debe a la falta de validación adecuada de una ruta proporcionada por el usuario antes de usarla en las operaciones con archivos. Un atacante puede aprovechar esta vulnerabilidad para eliminar archivos arbitrarios en el contexto del hipervisor. Era ZDI-CAN-12129.
CVE-2021-31420	Esta vulnerabilidad permite a los atacantes locales aumentar los privilegios en las instalaciones afectadas de Parallels Desktop 16.1.0-48950. Un atacante primero debe obtener la capacidad de ejecutar código con pocos privilegios en el sistema huésped de destino para aprovechar esta vulnerabilidad. La falla específica existe dentro del componente Toolgate. El problema se debe a la falta de una validación adecuada de la longitud de los datos proporcionados por el usuario antes de copiarlos en un búfer basado en pilas de longitud fija. Un atacante puede aprovechar esta vulnerabilidad para aumentar los privilegios y ejecutar código arbitrario en el contexto del hipervisor. Era ZDI-CAN-12220.
CVE-2021-31419	Esta vulnerabilidad permite a los atacantes locales revelar información confidencial sobre las instalaciones afectadas de Parallels Desktop 15.1.4-47270. Un atacante primero debe obtener la capacidad de ejecutar código con pocos privilegios en el sistema huésped de destino para aprovechar esta vulnerabilidad. La falla específica existe dentro del componente Toolgate. El problema se debe a la falta de inicialización adecuada de la memoria antes de acceder a ella. Un atacante puede aprovechar esto junto con otras vulnerabilidades para aumentar los privilegios y ejecutar código arbitrario en el contexto del hipervisor. Era ZDI-CAN-12136.
CVE-2021-31418	Esta vulnerabilidad permite a los atacantes locales revelar información confidencial sobre las instalaciones afectadas de Parallels Desktop 15.1.4-47270. Un atacante primero debe obtener la capacidad de ejecutar código con pocos privilegios en el sistema huésped de destino para aprovechar esta vulnerabilidad. La falla específica existe dentro del componente Toolgate. El problema se debe a la falta de inicialización adecuada de la memoria antes de acceder a ella. Un atacante puede aprovechar esto junto con otras vulnerabilidades para aumentar los privilegios y ejecutar código arbitrario en el contexto del hipervisor. Era ZDI-CAN-12221.
CVE-2021-31417	Esta vulnerabilidad permite a los atacantes locales revelar información confidencial sobre las instalaciones afectadas de Parallels Desktop 15.1.4-47270. Un atacante primero debe obtener la capacidad de ejecutar código con pocos privilegios en el sistema huésped de destino para aprovechar esta vulnerabilidad. La falla específica existe dentro del componente Toolgate. El problema se debe a la falta de inicialización adecuada de la memoria antes de acceder a ella. Un atacante puede aprovechar esto junto con otras vulnerabilidades para aumentar los privilegios y ejecutar código arbitrario en el contexto del hipervisor. Era ZDI-CAN-12131.
CVE-2021-30285	La validación incorrecta de la región de la memoria en Hypervisor puede conducir a una asignación de región incorrecta en Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking
CVE-2021-29795	IBM PowerVM Hypervisor FW860, FW930, FW940 y FW950 podrían permitir que un usuario local cree una secuencia especialmente diseñada de llamadas de hipervisor desde una partición que podría bloquear el sistema. Identificación de IBM X-Force: 203557.
CVE-2021-29765	IBM PowerVM Hypervisor FW940 y FW950 podrían permitir que un atacante obtenga información confidencial si obtiene acceso al servicio del FSP. Identificación de IBM X-Force: 202476.

CVE	Descripción
CVE-2021-28709	problemas con actualizaciones de P2M parcialmente exitosas en x86 Este registro de información de CNA se relaciona con múltiples CVE; el texto explica qué aspectos/vulnerabilidades corresponden a qué CVE.] Los huéspedes x86 HVM y PVH pueden iniciarse en modo PoD (populate-on-demand), para brindarles una forma de que más adelante se les asigne fácilmente más memoria. Los invitados pueden controlar ciertos aspectos P2M de páginas individuales a través de hiperllamadas. Estas hiperllamadas pueden actuar en rangos de páginas especificados a través de pedidos de páginas (lo que da como resultado un número de páginas de potencia de 2). En algunos casos, el hipervisor lleva a cabo las solicitudes dividiéndolas en partes más pequeñas. El manejo de errores en ciertos casos de PoD ha sido insuficiente porque, en particular, no se tuvo en cuenta correctamente el éxito parcial de algunas operaciones. Hay dos rutas de código afectadas: eliminación de página (CVE-2021-28705) e inserción de nuevas páginas (CVE-2021-28709). (Proporcionamos un parche que combina la solución a ambos problemas).
CVE-2021-28705	problemas con actualizaciones de P2M parcialmente exitosas en x86 Este registro de información de CNA se relaciona con múltiples CVE; el texto explica qué aspectos/vulnerabilidades corresponden a qué CVE.] Los huéspedes x86 HVM y PVH pueden iniciarse en modo PoD (populate-on-demand), para brindarles una forma de que más adelante se les asigne fácilmente más memoria. Los invitados pueden controlar ciertos aspectos P2M de páginas individuales a través de hiperllamadas. Estas hiperllamadas pueden actuar en rangos de páginas especificados a través de pedidos de páginas (lo que da como resultado un número de páginas de potencia de 2). En algunos casos, el hipervisor lleva a cabo las solicitudes dividiéndolas en partes más pequeñas. El manejo de errores en ciertos casos de PoD ha sido insuficiente porque, en particular, no se tuvo en cuenta correctamente el éxito parcial de algunas operaciones. Hay dos rutas de código afectadas: eliminación de página (CVE-2021-28705) e inserción de nuevas páginas (CVE-2021-28709). (Proporcionamos un parche que combina la solución a ambos problemas).
CVE-2021-28703	Las páginas de estado de la tabla de concesión v2 pueden permanecer accesibles después de la desasignación (toma dos) El invitado obtiene acceso permitido a ciertas páginas de memoria propiedad de Xen. La mayoría de dichas páginas permanecen asignadas/asociadas con un invitado durante toda su vida útil. Las páginas de estado de la tabla de concesión v2, sin embargo, se desasignan cuando un invitado cambia (regresa) de v2 a v1. La liberación de dichas páginas requiere que el hipervisor sepa en qué parte del invitado se asignaron estas páginas. El hipervisor rastrea solo un uso dentro del espacio de invitados, pero las solicitudes de carreras del invitado para insertar asignaciones de estas páginas pueden resultar en que cualquiera de ellas se asignen en múltiples ubicaciones. Al volver de v2 a v1, el invitado conservaría el acceso a una página que se liberó y quizás se reutilizó para otros fines. Este error se solucionó por casualidad mediante la limpieza del código en Xen 4.14,
CVE-2021-28701	Otra carrera en el manejo de XENMAPSPACE_grant_table Los invitados pueden acceder a ciertas páginas de memoria propiedad de Xen. La mayoría de dichas páginas permanecen asignadas/asociadas con un invitado durante toda su vida útil. Las páginas de estado de la tabla de concesión v2, sin embargo, se desasignan cuando un invitado cambia (hacia atrás) de v2 a v1. La liberación de tales páginas requiere que el hipervisor haga cumplir que ninguna solicitud paralela puede resultar en la adición de una asignación de dicha página a un invitado. Faltaba esa aplicación, lo que permitía a los invitados conservar el acceso a las páginas que se liberaron y quizás se reutilizaron para otros fines. Desafortunadamente, cuando se estaba preparando XSA-379, este problema similar no se notó.
CVE-2021-28698	bucles de ejecución prolongada en el manejo de la tabla de subvenciones Para monitorear correctamente el uso de recursos, Xen mantiene información sobre las asignaciones de concesión que un dominio puede crear para asignar las concesiones ofrecidas por otros dominios. En el proceso de llevar a cabo ciertas acciones, Xen iteraba sobre todas esas entradas, incluidas las que ya no están en uso y algunas que pueden haberse creado pero nunca se usaron. Si la cantidad de entradas para un dominio determinado es lo suficientemente grande, esta iteración de la tabla completa puede ocupar una CPU durante demasiado tiempo, privando a otros dominios o causando problemas en el propio hipervisor. Tenga en cuenta que un dominio puede mapear sus propias concesiones, es decir, aquí no es necesario que participen múltiples dominios. Sin embargo, un par de invitados que "cooperen" pueden causar que los efectos sean más severos.
CVE-2021-28697	Las páginas de estado de la tabla de concesión v2 pueden permanecer accesibles después de la desasignación. El invitado obtiene acceso permitido a ciertas páginas de memoria propiedad de Xen. La mayoría de dichas páginas permanecen asignadas/asociadas con un invitado durante toda su vida útil. Las páginas de estado de la tabla de concesión v2, sin embargo, se desasignan cuando un invitado cambia (regresa) de v2 a v1. La liberación de dichas páginas requiere que el hipervisor sepa en qué parte del invitado se asignaron estas páginas. El hipervisor rastrea solo un uso dentro del espacio de invitados, pero las

CVE	Descripción
	solicitudes de carreras del invitado para insertar asignaciones de estas páginas pueden resultar en que cualquiera de ellas se asignen en múltiples ubicaciones. Al volver de v2 a v1, el invitado conservaría el acceso a una página que se liberó y quizás se reutilizó para otros fines.
CVE-2021-27260	Esta vulnerabilidad permite a los atacantes locales revelar información confidencial sobre las instalaciones afectadas de Parallels Desktop 16.0.1-48919. Un atacante primero debe obtener la capacidad de ejecutar código con privilegios elevados en el sistema invitado de destino para aprovechar esta vulnerabilidad. La falla específica existe dentro del componente Toolgate. El problema se debe a la falta de una validación adecuada de los datos proporcionados por el usuario, lo que puede resultar en una lectura más allá del final de un búfer asignado. Un atacante puede aprovechar esto junto con otras vulnerabilidades para aumentar los privilegios y ejecutar código arbitrario en el contexto del hipervisor. Era ZDI-CAN-12068.
CVE-2021-27259	Esta vulnerabilidad permite a los atacantes locales aumentar los privilegios en las instalaciones afectadas de Parallels Desktop 16.0.1-48919. Un atacante primero debe obtener la capacidad de ejecutar código con pocos privilegios en el sistema huésped de destino para aprovechar esta vulnerabilidad. La falla específica existe dentro del componente Toolgate. El problema se debe a la falta de una validación adecuada de los datos proporcionados por el usuario, lo que puede provocar un desbordamiento de enteros antes de asignar un búfer. Un atacante puede aprovechar esta vulnerabilidad para aumentar los privilegios y ejecutar código arbitrario en el contexto del hipervisor. Era ZDI-CAN-12021.
CVE-2021-27244	Esta vulnerabilidad permite a los atacantes locales revelar información confidencial sobre las instalaciones afectadas de Parallels Desktop 16.0.1-48919. Un atacante primero debe obtener la capacidad de ejecutar código con pocos privilegios en el sistema huésped de destino para aprovechar esta vulnerabilidad. La falla específica existe dentro del componente Toolgate. El problema se debe a la falta de una validación adecuada de los datos proporcionados por el usuario, lo que puede resultar en una lectura más allá del final de un búfer asignado. Un atacante puede aprovechar esto junto con otras vulnerabilidades para aumentar los privilegios y ejecutar código arbitrario en el contexto del hipervisor. Era ZDI-CAN-11925.
CVE-2021-27243	Esta vulnerabilidad permite a los atacantes locales aumentar los privilegios en las instalaciones afectadas de Parallels Desktop 16.0.1-48919. Un atacante primero debe obtener la capacidad de ejecutar código con pocos privilegios en el sistema huésped de destino para aprovechar esta vulnerabilidad. La falla específica existe dentro del componente Toolgate. El problema se debe a la falta de una validación adecuada de los datos proporcionados por el usuario, lo que puede provocar un desbordamiento de enteros antes de asignar un búfer. Un atacante puede aprovechar esta vulnerabilidad para aumentar los privilegios y ejecutar código arbitrario en el contexto del hipervisor. Era ZDI-CAN-11924.
CVE-2021-27242	Esta vulnerabilidad permite a los atacantes locales aumentar los privilegios en las instalaciones afectadas de Parallels Desktop 16.0.1-48919. Un atacante primero debe obtener la capacidad de ejecutar código con pocos privilegios en el sistema huésped de destino para aprovechar esta vulnerabilidad. La falla específica existe dentro del componente Toolgate. El problema se debe a la falta de una validación adecuada de los datos proporcionados por el usuario, lo que puede provocar una condición de corrupción de la memoria. Un atacante puede aprovechar esta vulnerabilidad para aumentar los privilegios y ejecutar código en el contexto del hipervisor. Era ZDI-CAN-11926.
CVE-2021-26403	Las comprobaciones insuficientes en SEV pueden dar lugar a que un hipervisor malintencionado revele el secreto de lanzamiento, lo que podría poner en peligro la confidencialidad de la máquina virtual.
CVE-2021-26340	Un hipervisor malicioso junto con un proceso atacante sin privilegios dentro de una máquina virtual invitada SEV/SEV-ES puede fallar al vaciar el búfer de búsqueda de traducción (TLB), lo que resulta en un comportamiento inesperado dentro de la máquina virtual (VM).
CVE-2021-26311	En la función AMD SEV/SEV-ES, la memoria se puede reorganizar en el espacio de direcciones del invitado que no es detectado por el mecanismo de atestación que podría ser utilizado por un hipervisor malicioso para conducir potencialmente a la ejecución de código arbitrario dentro de la máquina virtual invitada si un administrador malintencionado tiene acceso para comprometer el hipervisor del servidor.
CVE-2021-22045	VMware ESXi (7.0, 6.7 antes de ESXi670-202111101-SG y 6.5 antes de ESXi650-202110101-SG), VMware Workstation (16.2.0) y VMware Fusion (12.2.0) contienen una vulnerabilidad de desbordamiento de almacenamiento dinámico en la emulación de dispositivos de CD-ROM. Un actor malicioso con acceso a una máquina virtual con

CVE	Descripción
	emulación de dispositivo de CD-ROM puede aprovechar esta vulnerabilidad junto con otros problemas para ejecutar código en el hipervisor desde una máquina virtual.
CVE-2021-21627	Una vulnerabilidad de falsificación de solicitud entre sitios (CSRF) en Jenkins Libvirt Agents Plugin 1.9.0 y versiones anteriores permite a los atacantes detener los dominios del hipervisor.
CVE-2021-20505	El protocolo de intercambio de claves de cifrado PowerVM Logical Partition Mobility (LPM) (PowerVM Hypervisor FW920, FW930, FW940 y FW950) puede verse comprometido. Si un atacante tiene la capacidad de capturar tráfico de red LPM cifrado y puede obtener acceso de servicio al FSP, puede usar esta información para realizar una serie de procedimientos de servicio de PowerVM para descifrar el tráfico de migración capturado ID de IBM X-Force: 198232
CVE-2021-1921	Posible corrupción de la memoria debido al manejo inadecuado de las operaciones de desmapeo del hipervisor para operaciones de memoria concurrentes en Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile

Nota: Autoría propia, basado en los Common Vulnerabilities and Exposures

Anexo 2

Tabla 2

Relación de amenazas y ataques por componentes

	Denegación de servicio VM	Software mal diseñado	Denegación de servicio al Hipervisor	Exploit a software de aplicaciones	Exploit a SO	Hyperjacking	Exploit Directo al hipervisor	Exploit al Firmware	Salto de máquina virtual	Monitoreo entre máquinas virtuales
Comprobación de tipos de variables en tiempo de ejecución	■	■		■						
Desbordamiento de memoria	■	■		■						
Inferencia del kernel en el espacio de usuario	■	■		■						
Fallo del software de desarrollo	■	■		■						
Control de acceso	■	■							■	
Posible inyección de código	■			■					■	
Concurencia de vulnerabilidad	■								■	
Error de resolución de dependencia		■		■						
Degradación del servicio durante la gestión										
Problema de configuración		■		■					■	
Criticidad del núcleo	■									
Mecanismos de seguridad no aplicables	■				■					
Acceso al espacio de usuario	■			■						
Exposición de hardware	■								■	
Co-residencia										■
Infraestructura de red común			■						■	■
Otros recursos compartidos			■						■	■
Compartir recursos con el anfitrión			■				■	■		
Implementación del método de virtualización							■			■
Supervisión del hipervisor						■				
Supervisión de la consola de administración	■		■							
Ejecución de VM no lineal		■								

Nota: Representa respectivamente ■ los componentes que son afectados.

Anexo 3

Tabla 3

Configuración de contramedidas para minimizar ataques.

Mecanismo	Contramedidas	Cobertura	Requisitos
Integración de Mecanismos de Seguridad en Tiempo de Diseño	Contador basado en la medida de kernel	kernel del sistema operativo, Kernel del sistema operativo host.	Existencia de implementaciones de mecanismos para los núcleos operados.
	Basado en aplicaciones.	Solicitud, tiempo de ejecución.	Existencia de implementaciones de mecanismos para todas las aplicaciones operadas y su tiempo de ejecución.
	Gestión de software seguro.	kernel del sistema operativo, Aplicación, tiempo de ejecución.	Gestión de software seguro solo para los administradores de paquetes.
	Entorno de ejecución.	Hipervisor, Kernel del sistema operativo host.	implementación de mecanismos en los hipervisores operados
	Granularidad del hipervisor.	Hipervisor.	Arquitectura modular del hipervisor.
	protección de Redes y Almacenamiento.	Hipervisor.	Dispositivos de almacenamiento y redes Interfaces del hipervisor.
	Verificación formal de Código.	Núcleo del sistema operativo, hipervisor, Kernel del sistema operativo host.	Base de código, diseño y mantenibilidad limitados al momento de la ejecución de pruebas.
Minimización de la superficie de ataque	Reducción de procesos innecesarios en el procesador.	Todos los componentes de software.	Diseño modular y soporte para deshabilitar características en tiempo de ejecución.
	Externalización de VM Gestión de software.	Aplicación, tiempo de ejecución, núcleo del sistema operativo.	Instancia de máquina virtual de corta duración, imagen protegida en el entorno de construcción.
	Seguimiento de recursos compartidos.	Aplicación, tiempo de ejecución, núcleo del sistema operativo.	Existencia de interfaces para monitorear y conocimiento necesario para el monitore de datos.
Adaptación basada en Seguridad Programabilidad	Controles de Seguridad a los Mecanismos.	Aplicación, tiempo de ejecución, núcleo del sistema operativo.	Especificación de los requisitos de seguridad y características del mecanismo.
	Programabilidad de seguridad.	Aplicación, tiempo de ejecución, núcleo del sistema operativo.	Interfaces de reconfiguración, o posibilidad de reiniciar componentes.

Nota: Configuración de contramedidas, basado del articulo Compastié (2020),