Alerta de seguridad cibernética	9VSA20-00324-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de noviembre de 2020
Última revisión	23 de noviembre de 2020

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información obtenida de VMware referente a múltiples vulnerabilidades que afectan a los productos VMware Horizon Server y Client, VMware SD-WAN Orchestrator, VMware ESXi, VMware Workstation Player/Pro, VMware Fusion/Pro y VMware Cloud Foundation. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidades

CVE-2020-3997
CVE-2020-3998
CVE-2020-3984
CVE-2020-3985
CVE-2020-4000
CVE-2020-4001
CVE-2020-4002
CVE-2020-4003
CVE-2020-4004
CVE-2020-4005

CVE-2020-3997

La aplicación no validaba correctamente algunos datos ingresados por el usuario, lo cual permitía a un atacante explotar la vulnerabilidad XSS (Cross-site Scripting) para inyectar código malicioso, el cual sería ejecutado por la aplicación.

Productos Afectados
Horizon Server versión 7.x para cualquier sistema operativo.

Mitigación
La vulnerabilidad fue mitigada en la versión 7.10.3 y 7.13.0 de Horizon Server.

Enlaces
https://www.vmware.com/security/advisories/VMSA-2020-0024.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3997

CVE-2020-3998

Debido a que la aplicación no validaba correctamente algunos datos ingresados por el usuario, un atacante podía extraer las credenciales hasheadas si es que el cliente fallaba.

Productos Afectados
Horizon Client versión 5.x y anteriores para el sistema operativo Windows.

Mitigación
La vulnerabilidad fue mitigada en la versión 5.5.0 de Horizon Client para Windows.

Enlaces
https://www.vmware.com/security/advisories/VMSA-2020-0024.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3998

CVE-2020-3984

El orquestador no aplica validaciones de datos ingresados por un usuario correctamente, permitiendo a un orquestador autenticado explotar las llamadas API vulnerables con consultas SQL especialmente diseñadas para obtener acceso a datos no autorizados.

Productos Afectados
SD-WAN Orchestrator versión 3.x.

Mitigación

La vulnerabilidad fue mitigada en las versiones 3.3.2 p3 compilación 3.3.2-GA-20201103 y 3.4.4 compilación R344-20201103-GA de SD-WAN Orchestrator.

Enlaces
https://www.vmware.com/security/advisories/VMSA-2020-0025.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3984

CVE-2020-4000

Es posible para un atacante realizar un ataque de directorio transversal, permitiéndole la ejecución de código remoto mediante la ejecución de archivos ubicados en los directorios.

Productos Afectados
SD-WAN Orchestrator versiones 4.x y 3.x para Linux.

Mitigación
La vulnerabilidad fue mitigada en las versiones 4.0.1, 3.3.2 p3 compilación 3.3.2-GA-20201103 y 3.4.4 compilación R344-20201103-GAde SD-WAN Orchestrator para Linux.

Enlaces
https://www.vmware.com/security/advisories/VMSA-2020-0025.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-4000

CVE-2020-4001

Las claves por defecto en el orquestador permiten a un atacante realizar un ataque “Pass-the-Hash” (en el que se utiliza un hash en vez de una clave para la autenticación). El mismo método “salt” es utilizado para las claves en sistemas recién instalados.

Productos Afectados
SD-WAN Orchestrator versiones 4.x y 3.x para Linux.

Mitigación
Para mitigar la vulnerabilidad, se debe cambiar las claves por defecto de las cuentas preconfiguradas en el SD-WAN Orchestrator antes del paso a producción.

Enlaces
https://www.vmware.com/security/advisories/VMSA-2020-0025.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-4001

CVE-2020-3985

El orquestador permite acceso para configurar niveles de permisos arbitrarios llevando a la escalación de privilegios, a través de llamadas a la API vulnerable.

Productos Afectados
SD-WAN Orchestrator versión 3.x para Linux.

Mitigación
La vulnerabilidad fue mitigada en las versiones 3.3.2 p3 compilación 3.3.2-GA-20201103 y 3.4.4 compilación R344-20201103-GAde SD-WAN Orchestrator para Linux.

Enlaces
https://www.vmware.com/security/advisories/VMSA-2020-0025.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3985

CVE-2020-4002

El orquestador maneja los parámetros de sistema de una forma insegura que permite a un atacante con privilegios altos ejecutar código arbitrario en el sistema operativo que aloja al orquestador.

Productos Afectados
SD-WAN Orchestrator versión 3.x para Linux.

Mitigación
La vulnerabilidad fue mitigada en las versiones 3.3.2 p3 compilación 3.3.2-GA-20201103 y 3.4.4 compilación R344-20201103-GAde SD-WAN Orchestrator para Linux.

Enlaces
https://www.vmware.com/security/advisories/VMSA-2020-0025.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-4002

CVE-2020-4003

Una vulnerabilidad de inyección de código SQL permitía obtener información no autorizada debido a la falta de validación de datos ingresados por el usuario en el sistema afectado.

Productos Afectados
SD-WAN Orchestrator versiones 4.x y 3.x para Linux.

Mitigación

La vulnerabilidad fue mitigada en las versiones 4.0.1, 3.3.2 p3 compilación 3.3.2-GA-20201103 y 3.4.4 compilación R344-20201103-GAde SD-WAN Orchestrator para Linux.

Enlaces
https://www.vmware.com/security/advisories/VMSA-2020-0025.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-4003

CVE-2020-4004

El controlador XHCI (USB 3.x) contiene una vulnerabilidad de uso de memoria después de ser liberada, lo que permitiría a un actor malicioso con privilegios administrativos locales en una máquina virtual, explotar esta vulnerabilidad para ejecutar código en el contexto del proceso VMX de la máquina virtual.

Productos Afectados
VMware ESXi versiones 7.0, 6.7 y 6.5.
VMware Fusion versión 11.x para OS X.
VMware Workstation versión 15.x.
VMware Cloud Foundation versiones 4.x y 3.x.

Mitigación
Para VMware ESXi, aplicar parche ESXi70U1b-17168206, ESXi670-202011101-SG o ESXi650-202011301-SG.
Para VMware Fusion, actualizar a la versión 11.5.7.
Para VMware Workstation, actualizar a la versión 11.5.7.
Para VMware Cloud Foundation (ESXi), el parche se encuentra pendiente aún.
Además se puede mitigar esta vulnerabilidad removiendo el controlador XHCI (USB 3.x).

Enlaces
https://www.vmware.com/security/advisories/VMSA-2020-0026.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-4004

CVE-2020-4005

Una vulnerabilidad de escalación de privilegios existe gracias a como ciertas llamadas de sistema son manejadas, un actor malicioso con privilegios en el proceso CMX podría escalar privilegios en el sistema afectado.

Productos Afectados
VMware ESXi versiones 7.0, 6.7 y 6.5.
VMware Cloud Foundation versiones 4.x y 3.x.

Mitigación

Para VMware ESXi, aplicar parche ESXi70U1b-17168206, ESXi670-202011101-SG o ESXi650-202011301-SG.
Para VMware Cloud Foundation (ESXi), el parche se encuentra pendiente aún.

Enlaces

https://www.vmware.com/security/advisories/VMSA-2020-0026.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-4005