Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°272	Fecha: 14-11-2023
		Página: 4 de 12

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Las vulnerabilidades en Citrix y VMWare están siendo explotadas activamente		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Las vulnerabilidades CitrixBleed CVE-2023-4966 en Citrix y CVE-2023-20867 / 34048 en VMWare están siendo explotadas para infectar a empresas con Ramsonware.

Citrix NetScaler es un dispositivo de red que proporciona servicios de equilibrio de carga, firewall y VPN. NetScaler Gateway generalmente se refiere a los componentes de autenticación y VPN, mientras que ADC se refiere a las funciones de administración de tráfico y equilibrio de carga.

vCenter Server es el centro de administración central para la suite vSphere de VMware y ayuda a los administradores a administrar y monitorear la infraestructura virtualizada.

2. DETALLES:

Citrix insta a sus clientes a aplicar correcciones para la CVE-2023-4966, que tiene una puntuación CVSS de 9.4 y afecta a NetScaler ADC y NetScaler Gateway. Esta vulnerabilidad crítica ha sido objeto de explotación activa, ya que se ha recibido informes creíbles de ataques dirigidos que aprovechan esta vulnerabilidad, corroborando un informe de Mandiant. Debido a la existencia de una PoC del exploit (llamada Citrix Bleed) es probable que aumente los esfuerzos de explotación en los próximos días.

Esta vulnerabilidad CVE-2023-4966 se describió como "divulgación de información confidencial".

Estas sesiones pueden persistir después de que se haya implementado la actualización para mitigar la vulnerabilidad. Además, se han observado secuestro de sesión en el que los datos de la sesión fueron robados antes de la implementación del parche y posteriormente utilizados por un actor de amenazas.

El secuestro de la sesión autenticada podría resultar en un mayor acceso posterior según los permisos y el alcance de acceso que se permitía a la identidad o sesión. Un actor de amenazas podría utilizar este método para recopilar credenciales adicionales, girar lateralmente y obtener acceso a recursos adicionales dentro de un entorno.

Las siguientes versiones de los dispositivos NetScaler ADC y Gateway se ven afectadas por la vulnerabilidad:

- NetScaler ADC y NetScaler Gateway 14.1 antes de 14.1-8.50
- NetScaler ADC y NetScaler Gateway 13.1 antes de 13.1-49.15
- NetScaler ADC y NetScaler Gateway 13.0 antes de 13.0-92.19
- NetScaler ADC 13.1-FIPS anterior a 13.1-37.164
- NetScaler ADC 12.1-FIPS anterior a 12.1-55.300
- NetScaler ADC 12.1-NDcPP anterior a 12.1-55.300

Por otra parte, VMware Tools contiene una vulnerabilidad de omisión de autenticación en el módulo vgauth.

El grupo de espionaje, rastreado como UNC3886 estaría abusando de esta falla de omisión de autenticación, identificada como CVE-2023-20867, de VMware Tools, para implementar las puertas traseras denominadas VirtualPita y VirtualPie en máquinas virtuales de ESXi comprometidas y que permiten obtener privilegios de root.

"Un host ESXi totalmente comprometido puede obligar a VMware Tools a no autenticar las operaciones del host, lo que afecta la confidencialidad y la integridad de la máquina virtual invitada", dijo VMware en un aviso de seguridad.

Si se explotara la vulnerabilidad, los atacantes instalan el malware utilizando paquetes de instalación de vSphere (VIB) malintencionados, paquetes diseñados para ayudar a los administradores a crear y mantener imágenes de ESXi. Una tercera cepa de malware (VirtualGate), que Mandiant detectó durante la investigación, actuó como un dropper que desofusca en memoria las cargas útiles de una DLL de segunda etapa en las máquinas virtuales secuestradas.

Productos afectados:

- Herramientas Vmware versión 10.3.x.
- Herramientas Vmware versión 11.xx.
- Herramientas Vmware versión 12.xx.

Además, VMware emitió actualizaciones de seguridad para corregir la vulnerabilidad de vCenter Server: CVE-2023-34048 de puntuación crítica, que puede explotarse teniendo acceso de red a vCenter Server, logrando desencadenar una escritura fuera de los límites en la implementación del protocolo DCERPC, que podría conducir a la ejecución remota de código en servidores vulnerables.

Los atacantes no autenticados pueden explotarlo de forma remota en ataques de baja complejidad que no requieren la interacción del usuario.

Los puertos de red específicos vinculados a una posible explotación en ataques dirigidos a esta vulnerabilidad son 2012/tcp, 2014/tcp y 2020/tcp.

Los productos afectados son:

- VMware vCenter Server versión 8.0
- VMware vCenter Server versión 7.0

3. RECOMENDACIONES:

- Actualizar el producto afectado a la última versión de software disponible para abordar la vulnerabilidad CVE-2023-4966. También se recomienda finalizar todas las sesiones después de la actualización y ejecutar el comando de la CLI: clear lb persistentSessions <vServer>.
- Actualizar a la versión 12.2.5 de VMware Tools para abordar la vulnerabilidad CVE-2023-20867.
- Actualizar a la versión 8.0U2 del Servidor VMware vCenter para abordar la vulnerabilidad CVE-2023-34048.

Fuente de Información:	• hxxps://enhacke.com/blog/vulnerabilidad-de-citrix-netscaler-parcheado-recientemente-explotado-como-zero-day-652ffb742c779 • hxxps://unaaldia.hispasec.com/2023/10/citrix-y-vmware-advierten-sobre-poc-de-exploits-relacionados-con-vulnerabilidades-criticas.html • hxxps://www.assetnote.io/resources/research/citrix-bleed-leaking-session-tokens-with-cve-2023-4966 • hxxps://blog.segu-info.com.ar/2023/10/zero-day-en-netscaler-adc-gateway.html • hxxps://blog.segu-info.com.ar/2023/06/zero-day-en-vmare-permite-instalar.html • hxxps://www.vmware.com/security/advisories/VMSA-2023-0013.html • hxxps://blog.segu-info.com.ar/2023/10/vulnerabilidad-critica-en-vmware.html • hxxps://www.vmware.com/security/advisories/VMSA-2023-0023.html

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°272**	**Fecha: 14-11-2023**
		Página: 9 de 12

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

Descripción

1. ANTECEDENTES:

Cisco ha reportado una vulnerabilidad de severidad **MEDIA** de tipo secuencias de comandos entre sitios (XSS) en la interfaz de administración basada en web de Cisco Integrated Management Controller (IMC). La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto ejecutar código de script arbitrario en el navegador del usuario objetivo o acceder a información confidencial basada en el navegador.

2. DETALLES:

La vulnerabilidad de severidad **media**, identificada por MITRE como CVE-2023-20228 de tipo XSS en la interfaz de administración basada en web de Cisco Integrated Management Controller, podría permitir a un atacante remoto no autenticado llevar a cabo un ataque de XSS contra un usuario de la interfaz.

Esta vulnerabilidad se debe a una validación insuficiente de la entrada del usuario. Un atacante podría aprovechar esta vulnerabilidad persuadiendo a un usuario de una interfaz afectada para que haga clic en un enlace manipulado. Un exploit exitoso podría permitir al atacante ejecutar código de script arbitrario en el navegador del usuario objetivo o acceder a información confidencial basada en el navegador.

A. Productos afectados:

Esta vulnerabilidad afecta a los siguientes productos de Cisco si ejecutan una versión vulnerable de Cisco IMC:

- Sistema informático de red empresarial (ENCS) serie 5000 versión 2.9 y anteriores, 3.1 y 3.2.
- Servidores en rack UCS Serie C M4 versión 4.1 y anteriores y M5 versión 4.1 y anteriores, 4.2 y 4.3.
- Servidores UCS Serie E M3 versión 3.2 y anteriores.
- Servidores de almacenamiento UCS serie S versión 4.2 y 4.3.

3. RECOMENDACIÓN:

- Actualizar los productos afectados con la última versión fija disponible. No existen soluciones alternativas que aborden esta vulnerabilidad.

Fuente de Información:	• hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-xss-UMYtYEtr