

Nro. Alerta:	EC-2022-59	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS <b>ALERTA DE SEGURIDAD</b>	
TLP:	 <b>TLP:BLANCO</b>		
Fecha:	08-abril-2022	<b>Vulnerabilidades en productos VMware</b>	Versión 1.0

## I. DATOS GENERALES:

<b>Clase de alerta:</b>	Vulnerabilidades
<b>Tipo de incidente:</b>	Sistema o Software Abierto
<b>Nivel de riesgo:</b>	Alto

## II. ALERTA

VMware dio a conocer diferentes vulnerabilidades calificadas como críticas, importantes y moderadas asociadas a varios productos disponibles en el mercado tecnológico.



Figura 1. Ilustración relacionada a VMware.  
Fuente: VMware

## III. INTRODUCCIÓN

VMware, a través de su Aviso de Seguridad VMSA-2022-0011; dio a conocer un total de ocho vulnerabilidades; cinco de ellas calificadas como críticas, dos con calificación de importante y una con calificación moderada. A continuación, se enumeran los CVE asociados.

ÍTEM	CVE ASOCIADO	Nivel de impacto
1	CVE-2022-22954	Crítico
2	CVE-2022-22955	Crítico
3	CVE-2022-22956	Crítico
4	CVE-2022-22957	Crítico
5	CVE-2022-22958	Crítico
6	CVE-2022-22959	Importante
7	CVE-2022-22960	Importante
8	CVE-2022-22961	Moderada

Tabla 1. CVE asociado a VMWARE  
Fuente: VMWARE

Nro. Alerta:	EC-2022-59	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS <b>ALERTA DE SEGURIDAD</b>	
TLP:	 <b>TLP:BLANCO</b>		
Fecha:	08-abril-2022	<b>Vulnerabilidades en productos VMware</b>	Versión 1.0

Estas vulnerabilidades se encuentran, asociadas a los siguientes productos:

- VMware Workspace ONE Access (Acceso)
- Administrador de identidades de VMware (vIDM)
- VMware vRealize Automatización (vRA)
- Fundación de la nube de VMware
- Administrador del ciclo de vida de vRealize Suite

#### IV. VECTOR DE ATAQUE:

En al siguiente tabla, se describe el vector de ataque asociado a estas vulnerabilidades.

Ítem	CVE asociado	Descripción Vector de Ataque	String Vector
1	CVE-2022-22954	Un actor malicioso con acceso a la red puede desencadenar una inyección de plantilla del lado del servidor que puede resultar en la ejecución remota de código.	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:X/RL:O/RC:C
2	CVE-2022-22955	Un actor malicioso puede eludir el mecanismo de autenticación y ejecutar cualquier operación debido a los puntos finales expuestos en el marco de autenticación.	
3	CVE-2022-22956	Un actor malicioso con acceso administrativo puede desencadenar la deserialización de datos que no son de confianza a través de un URI de JDBC malicioso, lo que puede provocar la ejecución remota de código.	
4	CVE-2022-22957	Un actor malicioso con acceso administrativo puede desencadenar la deserialización de datos que no son de confianza a través de un URI de JDBC malicioso, lo que puede provocar la ejecución remota de código.	CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:X/RL:O/RC:C
5	CVE-2022-22958	Un actor malicioso puede engañar a un usuario a través de una falsificación de solicitud entre sitios para validar involuntariamente un URI de JDBC malicioso.	
6	CVE-2022-22959	Un actor malicioso con acceso local puede escalar los privilegios a 'root'.	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:X/RL:O/RC:C
7	CVE-2022-22960	Un actor malintencionado con acceso remoto puede filtrar el nombre de host del sistema de destino. La explotación exitosa de este problema puede conducir a atacar a las víctimas.	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:X/RL:O/RC:C

**Tabla 2.** Vector de ataque de vulnerabilidades  
Fuente: VMWARE



Nro. Alerta:	EC-2022-59	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS <b>ALERTA DE SEGURIDAD</b>	
TLP:	 <b>TLP:BLANCO</b>		
Fecha:	08-abril-2022	<b>Vulnerabilidades en productos VMware</b>	Versión 1.0

## V. IMPACTO:

A continuación, se mencionan los impactos asociados a la vulnerabilidad en productos VMware.

Ítem	CVE asociado	Afectación	Impacto
1	CVE-2022-22954	Vulnerabilidad de ejecución remota de código de inyección de plantilla del lado del servidor	Confidencialidad: Alta Integridad: Alta Disponibilidad: Alta
2	CVE-2022-22955	Vulnerabilidades de omisión de autenticación OAuth2 ACS	
3	CVE-2022-22956		
4	CVE-2022-22957	Vulnerabilidades de ejecución remota de código de inyección	
5	CVE-2022-22958		
6	CVE-2022-22959	VMware corrigió errores de gravedad alta que podrían explotarse para ataques de falsificación de solicitudes entre sitios (CSRF)	Confidencialidad: Ninguna Integridad: En parte Disponibilidad: Ninguna
7	CVE-2022-22960	VMware corrigió errores de gravedad alta que podría provocar una escalada de privilegios.	Confidencialidad: Alta Integridad: Alta Disponibilidad: Alta
8	CVE-2022-22961	VMware también corrigió errores de gravedad media que permitiría obtener acceso a información sin autorización (CVE- 2022-22961).	Confidencialidad: En parte Integridad: Ninguna Disponibilidad: Ninguna

**Tabla 3.** Impacto de vulnerabilidades  
Fuente: Symantec

## VI. RECOMENDACIONES:

El EcuCert recomienda a su comunidad objetivo:

- Instalar las respectivas actualizaciones entregadas por el proveedor.
- Considerar la matriz de respuesta emitida por el fabricante, se sugiere revisar: <https://www.vmware.com/security/advisories/VMSA-2022-0011.html>



Nro. Alerta:	EC-2022-59	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS <b>ALERTA DE SEGURIDAD</b>	 <p>CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS <b>ECUCERT</b></p>
TLP:	 <b>TLP:BLANCO</b>		
Fecha:	08-abril-2022	<b>Vulnerabilidades en productos VMware</b>	Versión 1.0

## VII. REFERENCIAS:

VMware. (06 de 04 de 2022). *VMware Security Advisory*. Obtenido de VMware Security Advisory: <https://www.vmware.com/security/advisories/VMSA-2022-0011.html>

VMware. (s.f.). *VMware*. Obtenido de VMware: <https://www.vmware.com/latam.html>

VulDB. (07 de 04 de 2022). *VulDB*. Obtenido de VulDB: <https://vuldb.com/es/?id.196644>

VulDB. (7 de 04 de 2022). *VulDB*. Obtenido de VulDB: <https://vuldb.com/es/?id.196645>

VulDB. (7 de 04 de 2022). *VulDB*. Obtenido de VulDB: <https://vuldb.com/es/?id.196646>

VulDB. (07 de 04 de 2022). *VulDB*. Obtenido de VulDB: <https://vuldb.com/es/?id.196648>

VulDB. (7 de 04 de 2022). *VulDB*. Obtenido de VulDB: <https://vuldb.com/es/?id.196649>

VulDB. (07 de 04 de 2022). *VulDB*. Obtenido de VulDB: <https://vuldb.com/es/?id.196650>

