Nro. Alerta:	EC-2022-59	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	26-abril-2022	**Vulnerabilidades en productos VMware-Actualización**	Versión 1.1

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidades
Tipo de incidente: Sistema o Software Abierto
Nivel de riesgo: 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

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-59	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	26-abril-2022	**Vulnerabilidades en productos VMware-Actualización**	Versión 1.1

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		
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		
6	CVE-2022-22959	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.	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:X/RL:O/RC:C
7	CVE-2022-22960	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
8	CVE-2022-22961	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

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-59	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	26-abril-2022	**Vulnerabilidades en productos VMware-Actualización**	Versión 1.1

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. ACTUALIZACIÓN:

A partir de la fecha de la publicación del Aviso de Seguridad VMSA-2022-0011 publicado por VMware a inicio del abril de 2021; se han detectado nuevos ataques, aprovechando dichas vulnerabilidades.

Según información recolectada de fuentes abiertas, los diferentes actores de amenaza

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

explotan dichas vulnerabilidades para lanzar puertas traseras HTTPS inversas, balizas Cobalt Strike, Metasploit. A continuación, se enumeran las diferentes fases empleadas por los actores de amenaza:

FASE 1	• El acceso inicial se obtiene mediante la explotación de una vulnerabilidad de VMWare Identity Manager Service.
FASE 2	• Implementa un controlador de PowerShell y prepara el entorno para la siguiente etapa: "PowerTrash Loader".
FASE 3	• Se inyecta en la memoria un marco de prueba de penetración avanzado.

Tabla 4. Secuencia de ataque aprovechando vulnerabilidades de VMware
Fuente: Morpihsec

En la siguiente gráfica se muestra un esquema de aprovechamiento de vulnerabilidades.

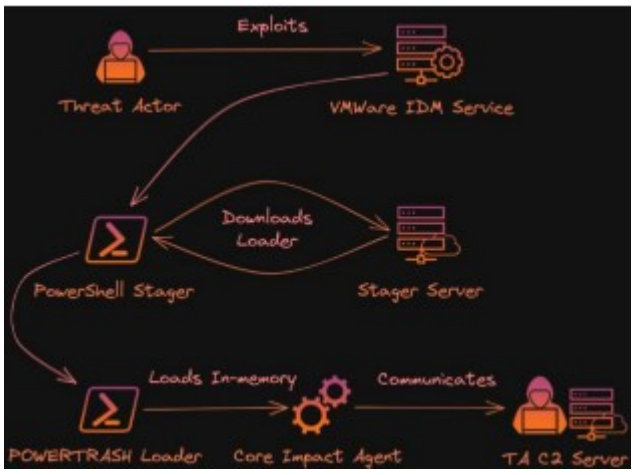

Figura 2. Ilustración relacionada a ataques en VMware.
Fuente: Morpihsec

Entre los Indicadores de Compromiso, se mencionan:

Parámetro	Detalle
Servidor C2	185[.]117[.]90[.]187 106[.]246[.]224[.]219
URL	hxxp://138[.]124[.]184[.]220/work_443.bin_m2.ps1
Hashes	746FFC3BB7FBE4AD229AF1ED9B6E1DB314880C0F9CB55AEC5F56DA79BCE2F79B 7BC14D231C92EEEB58197C9FCA5C8D029D7E5CF9FBFE257759F5C87DA38207D9

Tabla 5. IOC de ataques aprovechando vulnerabilidades de VMware.
Fuente: Morpihsec

VII. 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
- Emplear las protecciones del caso a los activos expuestos.

VIII. Descargo de responsabilidad

- La información en la presente alerta; se proporciona "tal cual" solo con fines informativos. EcuCERT no respalda ningún producto o servicio comercial, incluidos los sujetos de análisis.
- Cualquier referencia a productos, procesos o servicios comerciales específicos por marca de servicio, marca comercial, fabricante o de otro modo, no constituye ni implica respaldo, recomendación o favorecimiento por parte del EcuCERT.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

Toulas, B. (13 de 04 de 2022). *Bleppingcomputer*. Obtenido de Bleppingcomputer: https://www.bleepingcomputer.com/news/security/hackers-exploit-critical-vmware-

cve-2022-22954-bug-patch-now/

Vijayan, J. (25 de 04 de 2022). *DARK READING*. Obtenido de DARK READING: https://www.darkreading.com/attacks-breaches/-iranian-group-among-those-exploiting-recently-disclosed-rce-flaw-in-vmware

VMware. (06 de 04 de 2022). *VMware Security Advisoy*. Obtenido de VMware Security Advisoy: 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

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec