Nro. Alerta:	AL-2025-054	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	2-oct-2025	Vulnerabilidad Zero-Day en VMware Tools / Aria Operations (CVE-2025-41244)	Pág.: **1** of **5**

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad Zero-Day
Tipo de Incidente: Explotación local de privilegio / Explotación activa
Nivel de riesgo: Alta

II. ALERTA

Figura 1.- Vulnerabilidad Zero-Day en VMware Tools / Aria Operations (CVE-2025-41244) - figura referencial

Broadcom empresa propietaria de VMWare reveló una vulnerabilidad 0-day que permite a usuarios sin privilegios ejecutar código a nivel de root sin necesidad de autenticación, esta vulnerabilidad registrada como CVE-2025-41244 está siendo activamente explotada afectando a VMware Tools y VMware Aria Operations Discovery Management Pack (SDMP).

III. INTRODUCCIÓN

Las organizaciones que utilizan hipervisores VMWare enfrentan una nueva vulnerabilidad CVE-2025-41244, donde un usuario local sin privilegios que tenga acceso a una VM con VMWare Tools instalado y gestionadas por Aria Operations con SDMP habilitadas, puede escalar privilegios hasta ser un usuario root por medio del mecanismo de descubrimiento de servicios dentro de la misma VM.

El descubrimiento de servicios puede operar en dos modos:

Modo basado en credenciales: VMware Aria Operations ejecuta scripts de recopilación de métricas dentro de la VM invitada con las credenciales administrativas especificadas; VMware Tools actúa como proxy.

Modo sin credenciales: VMware Tools maneja la colección de métricas bajo su contexto privilegiado, sin necesidad de credenciales.

La empresa de Ciberseguridad NVISO, rastreo un actor de amenaza vinculado a China que Google Mandiant denomino UNC51744 (alias Uteus o Uetus), se cree que CVE-2025-41244 ha sido explotada desde octubre de 2024 y se desconoce si este exploit forma parte de las capacidades de UNC5174 o si el uso del 0-day fue accidental debido a su trivialidad.

IV. VECTOR DE ATAQUE

Broadcom ha evaluado la gravedad de este problema como importante con un nivel de severidad de 7.8 (Alta) y vector de ataque tipo local CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H.

CVE-2025-41244 existe para ambos modos, basado en credenciales y sin credenciales, dentro de los scripts de Aria Operations y dentro de las herramientas de Open source de VMware (open-vm-tools) respectivamente, esto debido a patrones de expresiones regulares demasiado amplios en el componente get-versions.sh.

Dentro de get-versions.sh, la función get_version() recorre los procesos con sockets de escucha y ejecuta los binarios coincidentes para recuperar la información de sus versiones.

Con el uso de expresiones regulares demasiada amplias (\S+) incluye involuntariamente directorios en los que el usuario puede escribir, como /tmp/httpd.

Esto permite a un atacante colocar binarios maliciosos en dichas ubicaciones y hacer que el contexto privilegiado de VMware lo ejecute y con ello el escalamiento de privilegios.

Ejemplos de llamadas vulnerables en **get-versions.sh**:

```
bash get_version "/\S+/(httpd-prefork|httpd|httpd2-prefork)($|\s)" -v
get_version "/\S+/mysqld($|\s)" -V
```

Figura 2.- Ejemplo de llamadas vulnerables en get-versions.sh - Vulnerabilidad Zero-Day en VMware Tools / Aria Operations (CVE-2025-41244)

Al imitar los binarios del sistema en rutas grabables, CVE-2025-41244 infringe CWE-426: Ruta de búsqueda no fiable, que es una vulnerabilidad de seguridad que ocurre cuando una aplicación utiliza una ruta de búsqueda no validada para localizar y cargar recursos externos (como bibliotecas dinámicas, ejecutables o scripts), permitiendo que un atacante ejecute código malicioso al colocar un archivo fraudulento en una ubicación que la aplicación busca antes que la ubicación legítima. Asi de esta forma ofrece oportunidades triviales de escalada de privilegios locales (LPE).

Un PoC (Prueba de Concepto) escrita en Go, demuestra la explotación, permite al atacante colocar un binario malicioso en un **path** coincidente al patrón de búsqueda (**/tmp/httpd** por ejemplo), luego cuando **get-versions.sh** lo invoca con -v, ese binario malicioso se ejecuta con privilegios del proceso de VMware Tools/SDMP, generando un shell root.

V. IMPACTO

Los productos y versiones afectados son los siguientes:

Productos	Componentes	Versiones	Corriendo en	Versión corre-gida
VMware Cloud Foundation VMware vSphere Foundation	VMware Cloud Founda-tion Operations	9.x.x.x	Any	9.0.1.0
VMware Cloud Foundation VMware vSphere Foundation	VMware Tools	13.x.x.x	Windows, Linux	13.0.5.0
VMware Aria Operations	VMware Aria Operations	8.x	Any	8.18.5
VMware Tools	N/A	13.x.x	Windows, Linux	13.0.5
VMware Tools	N/A	12.x.x, 11. x.x	Windows, Linux	12.5.4
VMware Cloud Foundation	VMware Aria Operations	5.x, 4.x	Any	KB92148
VMware Telco Cloud Platform	VMware Aria Operations	5.x, 4.x	Any	8.18.5
VMware Telco Cloud Infras-tructure	VMware Aria Operations	3.x, 2.x	Any	8.18.5

Tabla 1.- Productos, Versiones afectadas y corregidas - Vulnerabilidad Zero-Day en VMware Tools / Aria Operations (CVE-2025-41244)

VI. INDICADORES DE COMPROMISO

- vmtoolsd – Proceso legítimo de VMware Tools que es abusado para cargar o ejecutar binarios maliciosos.
- /tmp/httpd – Ruta sospechosa usada por el atacante para alojar binarios maliciosos. El uso del directorio /tmp es típico en ataques para alojar o ejecutar código temporalmente.

VII. RECOMENDACIONES:

- Aplicar los parches publicados por Broadcom / VMware inmediatamente. [6]
- Deshabilitar temporalmente la función SDMP (Service Discovery Management Pack) si no es crítica para operaciones.
- Monitorear actividad anómala: detectar procesos hijos inesperados del servicio vmtoolsd o ejecución de binarios inusuales desde directorios temporales.
- Restringir permisos de escritura en directorios temporales (por ejemplo /tmp) dentro de las máquinas virtuales.
- Revisar y reforzar controles internos de acceso a VM para evitar que usuarios no privilegiados puedan ejecutar código arbitrario.
- Auditar periódicamente el entorno virtual para detectar persistencias o modificaciones sospechosas.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

SECURITYWEEK (2025). Broadcom Fails to Disclose Zero-Day Exploitation of VMware Vulnerability. https://www.securityweek.com/broadcom-fails-to-disclose-zero-day-exploitation-of-vmware-vulnerability/

GBHACKERS (2025). VMware Tools and Aria 0-Day. https://gbhackers.com/vmware-tools-and-aria-0-day/

CYBERPRESS (2025). VMware Tools & Aria 0-Day Exploitation. https://cyberpress.org/vmware-tools-aria-0-day/

SECURITYAFFAIRS (2025). Broadcom Patches VMware Zero-Day Actively Exploited by UNC5174.https://securityaffairs.com/182816/uncategorized/broadcom-patches-vmware-zero-day-actively-exploited-by-unc5174.html

SOCPRIME (2025). CVE-2025-41244 Zero-Day Vulnerability. https://socprime.com/blog/cve-2025-41244-zero-day-vulnerability/?utm_source

CVE (2025). CVE-2025-41244. https://www.cve.org/CVERecord?id=CVE-2025-41244

QUALYS THREATPROTECT / BROADCOM (2025). Broadcom Addresses Actively Exploited Vulnerability in VMware Aria Operations and VMware Tools (CVE-2025-41244). https://threatprotect.qualys.com/2025/10/01/broadcom-addresses-actively-exploited-vulnerability-in-vmware-aria-operations-and-vmware-tools-cve-2025-41244/

THE HACKER NEWS (2025). Urgent: China-Linked Hackers Exploit New VMware Zero-Day. https://thehackernews.com/2025/09/urgent-china-linked-hackers-exploit-new.html

CYBERSECURITY HELP (2025). VMware Tools / Aria 0-Day Exploit. https://www.cybersecurity-help.cz/blog/4982.html?utm_source

TECHRADAR (2025). Broadcom Finally Patches Dangerous VMware Zero-Day Exploited by Chinese Hackers. https://www.techradar.com/pro/security/broadcom-finally-patches-dangerous-vmware-zero-day-exploited-by-chinese-hackers?utm_source