Nro. Alerta:	AL-2025-008	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	26-feb-2025	Radiant DICOM Viewer (CVE-2025-1001)	Pág.: **1** of **4**

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Nivel de riesgo: Media

II. ALERTA

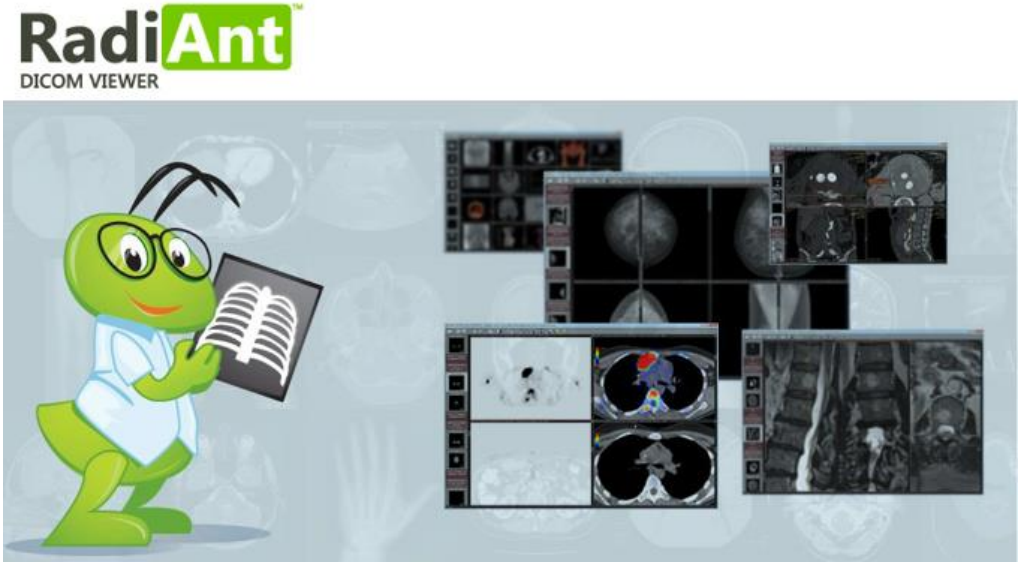


Figura 1 *Radiant DICOM Viewer – figura referencial*

Se ha detectado la vulnerabilidad CVE-2025-1001 en RadiAnt DICOM Viewer versión 2024.02 que permite ataques MITM debido a una validación inadecuada de certificados en el proceso de actualización.

III. INTRODUCCIÓN

RadiAnt DICOM Viewer, es un programa que permite visualizar imágenes médicas ejecutando desplazamientos y zoom de fluidos, ajuste de brillo y contraste, rotación de imágenes, longitud de segmentos, entre otros, en formato DICOM (Digital Imaging and Communications in Medicine) soporta muchos tipos de imágenes como: Monocromáticas (ej. CR, CT, MR), a color (ej. US, reconstrucciones 3D), Imágenes estáticas (ej. CR, MR, CT), secuencias dinámicas (ej. XA, US), sin comprimir y comprimidas (RLE, JPEG con pérdida, JPEG sin pérdida, JPEG 2000).

La actualización remota de RadiAnt DICOM Viewer no verifica de manera suficiente la legitimidad del certificado del servidor (este tipo de vulnerabilidades está documentado bajo cwe-295: Improper Certificate Validation).

La falla en el mecanismo de actualización permite a un atacante interceptar y manipular el proceso de verificación de certificados mediante un ataque Men-in-the-middle para poder modificar la respuesta del servidor y entregar actualizaciones maliciosas con el fin de comprometer la integridad del sistema y del usuario.

IV. VECTOR DE ATAQUE

En base a CVSS v4 se ha calculado una puntuación de 5.7 del tipo AV: A (Adyacente), donde un atacante explota la vulnerabilidad sólo a través de una red física compartida.

V. IMPACTO

Radiant DICOM Viewer está construido y probado específicamente para la plataforma Windows, la investigación reciente ha determinado que la vulnerabilidad se encuentra en la versión 2024.02 del software y aunque el objetivo inmediato es el visor DICOM, las implicaciones se extienden a cualquier organización que dependa de procesos seguros de imágenes médicas digitales. Los sectores de la atención sanitaria y la salud pública son especialmente sensibles debido a la naturaleza crítica de los datos y servicios que manejan.

Proveedores de atención médica: donde la integridad inmediata de los datos es esencial.

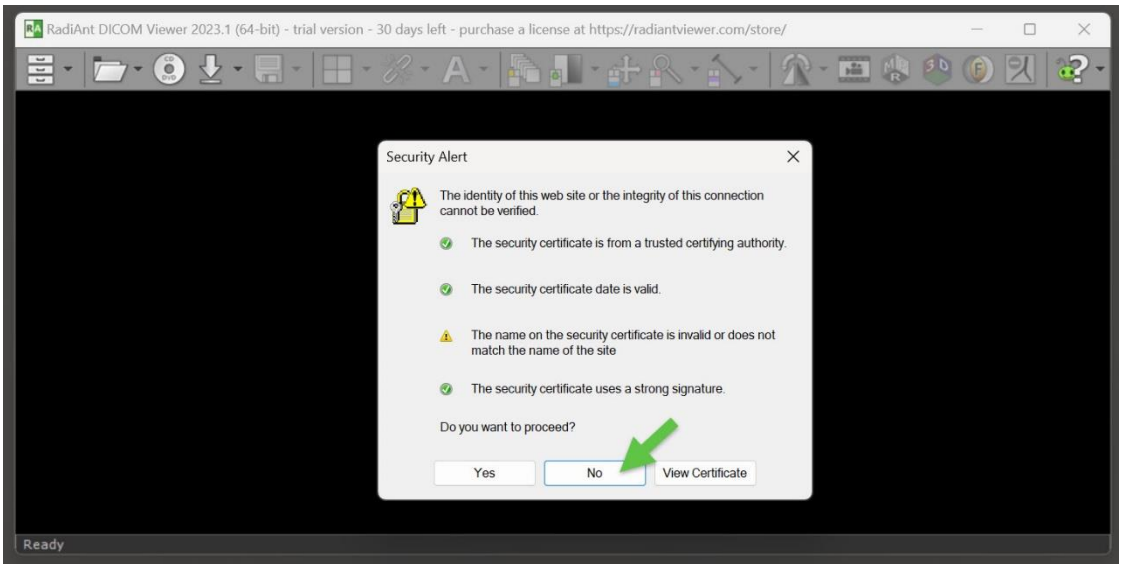
Organizaciones de salud pública: confíe en sistemas fiables para obtener diagnósticos precisos.

Implementación global: con instalaciones implementadas en todo el mundo, el impacto potencial es amplio.

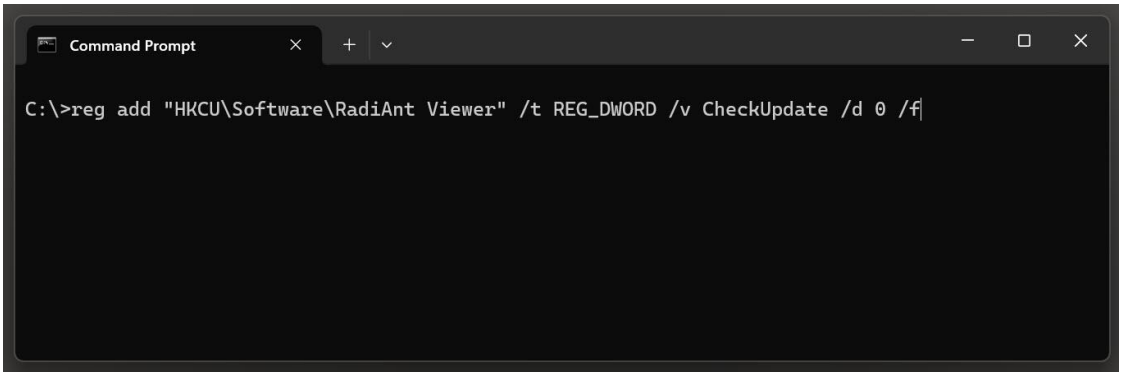
VI. RECOMENDACIONES:

- Todos los usuarios con un plan de suscripción activo pueden descargar e instalar la versión parcheada 2025.1 desde el sitio web oficial: Descargar RadiAnt DICOM Viewer 2025.1
- Los usuarios con licencias permanentes y soporte vencido, o aquellos con un plan de suscripción que prefieren permanecer en una versión más antigua, pueden mitigar el riesgo siguiendo estas precauciones:

  a) No continúe si aparece un cuadro de diálogo de alerta de seguridad del certificado. Haga clic en "No" cuando se le solicite.



b) Deshabilite las notificaciones de actualización automática mediante este comando:
reg add "HKCU\Software\RadiAnt Viewer" /t REG_DWORD /v CheckUpdate /d 0 /f



- Evite buscar actualizaciones manualmente ("Buscar actualizaciones ahora" en el menú de la barra de herramientas).
- Ignore cualquier contenido que se muestre en la ventana de verificación de actualización y ciérrela inmediatamente si aparece.
- Evite utilizar redes que no sean de confianza, incluidas las redes wifi públicas. El uso de su dispositivo en una red que no sea de confianza aumenta las posibilidades de ser víctima de un ataque MITM.

VII. 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.

VIII. REFERENCIAS:

https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2025-1001

https://www.radiantviewer.com/

https://www.cve.org/CVERecord?id=CVE-2025-1001

https://www.radiantviewer.com/c/security-advisory-cve-2025-1001/

https://nvd.nist.gov/vuln/detail/CVE-2025-1001