

Alerta ID:	121
Fecha del reporte:	08/07/2026
Entidad:	Todas las entidades del ecosistema digital
Título:	CVE-2026-8451 – Citrix NetScaler ADC / NetScaler Gateway
Herramienta de detección	N/A
Activo involucrado:	Autenticación SAML. Dark Reading
Tipo de alerta:	Alerta
Nivel de riesgo:	Alto

Objetivo:

Informar a las organizaciones del sector salud en Colombia sobre la identificación de la vulnerabilidad de seguridad **CVE-2026-8451**, que afecta a los productos **Citrix NetScaler ADC y NetScaler Gateway** cuando se encuentran configurados como proveedores de identidad **SAML Identity Provider (SAML IdP)**. Esta falla, clasificada como una vulnerabilidad de lectura fuera de límites (*Out-of-Bounds Read*), podría permitir a un atacante remoto no autenticado acceder a información almacenada temporalmente en memoria del dispositivo, incluyendo datos asociados a procesos de autenticación, sesiones activas o información sensible del entorno, comprometiendo la confidencialidad, integridad y seguridad de los servicios tecnológicos que soportan los procesos asistenciales y administrativos del sector salud.



El propósito de esta alerta es que las organizaciones del sector salud validen si dentro de su infraestructura tecnológica, servicios tercerizados o soluciones administradas por proveedores externos utilizan dispositivos **Citrix NetScaler ADC o NetScaler Gateway** en versiones afectadas, especialmente aquellos expuestos a internet y utilizados para acceso remoto, publicación de aplicaciones institucionales, conexiones VPN, mecanismos de autenticación única (SSO) o acceso seguro a plataformas críticas. Esta validación debe contemplar la revisión del inventario tecnológico, identificación de versiones instaladas, análisis de configuraciones SAML habilitadas, revisión de registros de autenticación y aplicación oportuna de las actualizaciones de seguridad recomendadas, con el fin de reducir riesgos que puedan afectar sistemas clínicos, administrativos, plataformas de historia clínica electrónica, servicios de laboratorio, telemedicina y demás componentes esenciales para la continuidad operativa de las instituciones de salud.

Descripción:

Citrix ha publicado actualizaciones de seguridad para corregir la vulnerabilidad identificada como **CVE-2026-8451**, que afecta a los productos **Citrix NetScaler ADC y NetScaler Gateway** cuando se encuentran configurados como **proveedores de identidad SAML (SAML Identity Provider - IdP)**. Esta falla corresponde a una vulnerabilidad de lectura fuera de límites (*Out-of-Bounds Read*) en el procesamiento de solicitudes de autenticación SAML, situación que podría permitir a un atacante remoto no autenticado acceder a información almacenada temporalmente en la memoria del dispositivo, comprometiendo la confidencialidad de datos relacionados con sesiones, procesos de autenticación y elementos sensibles del entorno tecnológico.



La vulnerabilidad se presenta debido a una validación insuficiente durante el procesamiento de determinados datos enviados al componente encargado de gestionar autenticaciones SAML. Un atacante podría aprovechar esta condición mediante solicitudes especialmente diseñadas dirigidas al dispositivo NetScaler expuesto, con el objetivo de obtener información de memoria que podría incluir datos asociados a mecanismos de autenticación, tokens de sesión u otra información utilizada durante la operación del servicio. Esta situación representa un riesgo significativo para las organizaciones del sector salud debido a que estos dispositivos suelen utilizarse como puntos de acceso seguro para usuarios internos, proveedores externos, profesionales asistenciales y aplicaciones críticas.

El impacto potencial de esta vulnerabilidad es especialmente relevante en instituciones de salud que utilizan **Citrix NetScaler Gateway** para habilitar conexiones remotas, acceso VPN, publicación de aplicaciones institucionales, autenticación única (SSO) o conexión hacia plataformas misionales como sistemas de historia clínica electrónica, laboratorios, servicios administrativos y herramientas de telemedicina. Una explotación exitosa podría facilitar accesos no autorizados, exposición de información sensible o servir como punto inicial para ataques posteriores contra otros componentes de la infraestructura tecnológica.

Las actualizaciones de seguridad publicadas por Citrix corrigen esta condición fortaleciendo los mecanismos de validación y procesamiento de solicitudes SAML, reduciendo la posibilidad de acceso indebido a información almacenada en memoria. Se recomienda a las organizaciones del sector salud validar inmediatamente la presencia de versiones afectadas, actualizar los dispositivos NetScaler a versiones corregidas, revisar configuraciones de autenticación habilitadas y analizar registros de actividad sospechosa, debido a que la explotación de esta vulnerabilidad podría afectar la seguridad de los accesos remotos y la continuidad de servicios tecnológicos esenciales para la operación sanitaria.



Consecuencias de la explotación

La explotación exitosa de la vulnerabilidad **CVE-2026-8451** en **Citrix NetScaler ADC y NetScaler Gateway** puede generar consecuencias significativas a nivel técnico, operativo y de seguridad de la información para las organizaciones del sector salud. Debido a que estos dispositivos suelen operar como puntos de acceso para usuarios internos, proveedores externos y aplicaciones críticas, una explotación podría afectar la protección de los servicios tecnológicos que soportan los procesos asistenciales y administrativos. Entre las principales consecuencias se destacan las siguientes:

1. Exposición de información sensible de autenticación:

Los atacantes que aprovechen esta vulnerabilidad podrían acceder a información almacenada temporalmente en la memoria del dispositivo, incluyendo datos asociados a procesos de autenticación SAML, sesiones activas, tokens o información utilizada durante la validación de usuarios, comprometiendo la confidencialidad de los mecanismos de acceso institucional.

2. Compromiso de accesos remotos y servicios publicados:

La explotación de la vulnerabilidad podría afectar dispositivos utilizados como puerta de entrada para conexiones VPN, escritorios remotos, aplicaciones institucionales y servicios publicados hacia internet, aumentando el riesgo de accesos no autorizados a plataformas utilizadas por personal médico, administrativo o proveedores tecnológicos.

3. Robo o reutilización de información de sesión:

La información obtenida mediante la lectura indebida de memoria podría ser utilizada por actores maliciosos para intentar reutilizar elementos de autenticación, evadir controles de



acceso o realizar actividades no autorizadas dentro de los servicios protegidos por NetScaler, afectando la seguridad de usuarios y sistemas conectados.

4. Compromiso de infraestructura tecnológica crítica:

Un dispositivo NetScaler comprometido podría convertirse en un punto inicial para ataques posteriores contra otros componentes de la infraestructura institucional, incluyendo servidores internos, aplicaciones clínicas, sistemas de historia clínica electrónica, plataformas administrativas, bases de datos y servicios utilizados para la operación hospitalaria.

5. Interrupción de servicios esenciales:

La afectación de los mecanismos de acceso remoto o publicación de aplicaciones podría ocasionar indisponibilidad temporal de servicios tecnológicos necesarios para la atención en salud, impactando procesos como consulta de información clínica, gestión administrativa, comunicación interna o acceso de proveedores autorizados.

6. Riesgos reputacionales y de confianza institucional:

Un incidente asociado al compromiso de plataformas de acceso seguro podría afectar la confianza de pacientes, colaboradores, proveedores y entidades reguladoras, especialmente si deriva en exposición de información sensible o afectación de la continuidad operativa de los servicios de salud.

7. Impacto regulatorio y cumplimiento normativo:

Las organizaciones que presenten exposición de información personal o datos sensibles de pacientes como consecuencia de una explotación podrían enfrentar requerimientos, investigaciones o sanciones relacionadas con el incumplimiento de medidas de seguridad y



protección de datos personales, conforme a la **Ley 1581 de 2012** en Colombia y demás normativas aplicables sobre privacidad y seguridad de la información.

Modo de explotación del ataque

La explotación de la vulnerabilidad **CVE-2026-8451** en **Citrix NetScaler ADC y NetScaler Gateway** puede llevarse a cabo mediante una serie de fases que permiten a un atacante remoto aprovechar debilidades en el procesamiento de solicitudes de autenticación SAML cuando el dispositivo se encuentra configurado como **Proveedor de Identidad SAML (SAML IdP)**:

Fase 1 – Identificación de dispositivos vulnerables y reconocimiento del servicio expuesto

El ataque inicia cuando el actor malicioso realiza actividades de reconocimiento para identificar organizaciones que utilizan dispositivos **Citrix NetScaler ADC o NetScaler Gateway** expuestos a internet y configurados con funciones de autenticación SAML. Mediante técnicas de escaneo y análisis de servicios publicados, el atacante puede determinar versiones vulnerables del dispositivo, configuraciones habilitadas y posibles puntos de entrada para realizar intentos de explotación.

Fase 2 – Envío de solicitudes SAML manipuladas y explotación de la vulnerabilidad

Una vez identificado un dispositivo vulnerable, el atacante puede enviar solicitudes especialmente diseñadas hacia el componente encargado del procesamiento de autenticaciones SAML. Debido a una validación insuficiente en el manejo de determinados datos, la vulnerabilidad de lectura fuera de límites (*Out-of-Bounds Read*) podría permitir el acceso no autorizado a información almacenada temporalmente en la memoria del dispositivo.

Fase 3 – Obtención de información sensible y afectación de mecanismos de autenticación



Tras explotar la vulnerabilidad, el atacante podría obtener información contenida en memoria relacionada con procesos de autenticación, sesiones activas, tokens u otros datos utilizados por el servicio. Esta información podría ser analizada para intentar comprometer accesos legítimos, evadir controles de seguridad o acceder a recursos protegidos por el dispositivo NetScaler.

Fase 4 – Movimiento lateral y compromiso de servicios internos

Con información obtenida del dispositivo comprometido, el atacante podría intentar ampliar su alcance dentro de la infraestructura tecnológica de la organización, aprovechando los accesos remotos, conexiones VPN o aplicaciones publicadas mediante NetScaler. Esto podría facilitar intentos de acceso hacia sistemas críticos como plataformas de historia clínica electrónica, servidores administrativos, bases de datos o servicios utilizados por proveedores externos.

Fase 5 – Persistencia, ocultamiento y continuidad del ataque

Luego de obtener acceso o información relevante, el atacante podría realizar actividades orientadas a mantener presencia dentro del entorno comprometido, modificar configuraciones, aprovechar credenciales obtenidas o utilizar otros vectores de ataque disponibles. La falta de monitoreo adecuado de registros de autenticación, accesos remotos y eventos de seguridad podría permitir que estas actividades permanezcan ocultas durante periodos prolongados, incrementando el impacto sobre la infraestructura tecnológica del sector salud.

Vulnerabilidades asociadas

- La vulnerabilidad **CVE-2026-8451** en **Citrix NetScaler ADC y NetScaler Gateway** no depende de fallos externos en otros componentes tecnológicos, sino que se origina por debilidades propias en el procesamiento y validación de solicitudes de autenticación **SAML**



dentro del dispositivo. Sin embargo, su explotación puede verse favorecida por configuraciones expuestas, versiones desactualizadas y una gestión inadecuada de los mecanismos de autenticación utilizados en estos servicios.

- **Fallas en la validación de memoria y procesamiento de solicitudes SAML:** La vulnerabilidad corresponde a una condición de lectura fuera de límites (*Out-of-Bounds Read*) causada por un manejo incorrecto de determinados datos durante el procesamiento de solicitudes SAML. Esta debilidad podría permitir que un atacante remoto no autenticado acceda a información almacenada temporalmente en la memoria del dispositivo, comprometiendo la seguridad de los procesos de autenticación.

- **Configuraciones inseguras o exposición innecesaria del servicio:** Los dispositivos NetScaler ADC y NetScaler Gateway que se encuentran publicados directamente hacia internet, especialmente aquellos utilizados como proveedores de identidad SAML, aumentan la superficie de ataque disponible. Una configuración inadecuada, falta de segmentación o exposición de servicios no requeridos puede facilitar las actividades de reconocimiento y explotación por parte de actores maliciosos.

- **Compromiso de mecanismos de autenticación y control de acceso:** La información obtenida mediante la explotación de la vulnerabilidad podría incluir elementos asociados a sesiones activas, tokens de autenticación u otros datos temporales utilizados por el sistema. Esto podría



permitir intentos de reutilización de sesiones, afectación de controles de acceso o comprometer la seguridad de usuarios que utilizan servicios protegidos mediante NetScaler.

- **Ausencia de controles complementarios de monitoreo y protección:** La falta de medidas adicionales como autenticación multifactor (MFA), monitoreo continuo de accesos remotos, análisis de registros, restricción de privilegios administrativos y aplicación oportuna de actualizaciones incrementa el riesgo de impacto. Estas deficiencias podrían facilitar que un atacante mantenga actividades no autorizadas dentro del entorno tecnológico, afectando la confidencialidad, integridad y disponibilidad de la información gestionada por las organizaciones del sector salud.

Recomendaciones de detección y mitigación

Los equipos de seguridad, infraestructura y administración de TI en las organizaciones del sector salud deben priorizar la **identificación, actualización y aseguramiento de los dispositivos Citrix NetScaler ADC y NetScaler Gateway** que se encuentren implementados dentro de la infraestructura tecnológica institucional, especialmente aquellos expuestos a internet o configurados como proveedores de identidad **SAML (SAML Identity Provider)**. Se recomienda verificar todos los dispositivos físicos, virtuales y servicios administrados por terceros, incluyendo ambientes de producción, pruebas,



contingencia y recuperación ante desastres, con el objetivo de identificar versiones vulnerables y evitar posibles escenarios de explotación.

Adicionalmente, se recomienda realizar un inventario técnico de todos los componentes que utilicen **Citrix NetScaler** como mecanismo de acceso remoto, publicación de aplicaciones o autenticación centralizada. Este inventario debe incluir versiones instaladas, configuraciones habilitadas, servicios publicados, integraciones SAML activas, usuarios administrativos, accesos externos autorizados y proveedores tecnológicos con conexión hacia la infraestructura institucional.

Entre las medidas prioritarias se recomienda aplicar las siguientes:

1. Actualizar inmediatamente los dispositivos NetScaler afectados:

Aplicar las versiones corregidas publicadas por Citrix para **NetScaler ADC y NetScaler Gateway**, asegurando que los dispositivos operen con versiones soportadas y libres de la vulnerabilidad CVE-2026-8451. Se debe evitar mantener versiones antiguas en ambientes productivos, contingencia o pruebas que puedan convertirse en puntos de entrada para atacantes.

2. Validar configuraciones SAML habilitadas:



Revisar los dispositivos configurados como **SAML Identity Provider**, ya que la vulnerabilidad afecta específicamente esta funcionalidad. Se recomienda validar integraciones activas, certificados asociados, configuraciones de autenticación y servicios que dependan de estos mecanismos para controlar accesos.

3. Reducir la superficie de exposición externa:

Limitar la publicación de servicios NetScaler únicamente a los requerimientos necesarios, aplicando controles como segmentación de red, listas de acceso, restricción de direcciones IP autorizadas y revisión periódica de servicios expuestos hacia internet.

4. Fortalecer los controles de autenticación y acceso:

Implementar mecanismos adicionales como autenticación multifactor (MFA), políticas de mínimo privilegio, revisión periódica de cuentas administrativas y eliminación de accesos innecesarios, reduciendo el impacto potencial ante un compromiso del dispositivo.

5. Fortalecer la instrumentación y monitoreo de eventos de seguridad:

Revisar registros (*logs*) de NetScaler relacionados con autenticaciones, solicitudes SAML, accesos administrativos y conexiones remotas.



Identificar patrones anómalos como múltiples intentos de autenticación fallidos, accesos desde ubicaciones inusuales o solicitudes sospechosas hacia servicios publicados.

Analizar eventos de seguridad asociados a sesiones, tokens o accesos remotos que puedan indicar intentos de explotación.

6. Realizar análisis de compromiso posterior a la actualización:

En caso de identificar versiones vulnerables expuestas a internet, se recomienda realizar una revisión preventiva de indicadores de compromiso, incluyendo análisis de registros históricos, accesos privilegiados, sesiones activas, cambios de configuración no autorizados y comportamiento anómalo del dispositivo.

7. Gestionar accesos de proveedores y terceros tecnológicos:

Validar conexiones realizadas por proveedores externos mediante NetScaler Gateway, verificando que cuenten con controles adecuados, accesos temporales, trazabilidad de actividades y mecanismos de autenticación segura, evitando que una cuenta comprometida de terceros sea utilizada como vía de ingreso a la infraestructura institucional.

8. Validar despliegues corporativos y ambientes distribuidos:



Para organizaciones con múltiples sedes, hospitales, clínicas o centros de atención que utilicen diferentes dispositivos NetScaler, se debe garantizar que las actualizaciones y configuraciones de seguridad sean aplicadas de manera uniforme, evitando que equipos rezagados permanezcan expuestos y puedan comprometer la seguridad general de la organización.

Recomendaciones de prevención y mitigación

Para prevenir la explotación de la vulnerabilidad **CVE-2026-8451** y fortalecer la seguridad de los dispositivos **Citrix NetScaler ADC y NetScaler Gateway** utilizados en las organizaciones del sector salud, se recomienda implementar las siguientes medidas de prevención, actualización y fortalecimiento de controles de seguridad:

1. Aplicar las actualizaciones de seguridad inmediatamente:

Las organizaciones deben actualizar los dispositivos **Citrix NetScaler ADC y NetScaler Gateway** a las versiones corregidas proporcionadas por el fabricante, verificando que los ambientes de producción, pruebas, contingencia y recuperación ante desastres no mantengan versiones vulnerables. Se debe priorizar la actualización de aquellos dispositivos expuestos a internet o utilizados para acceso remoto, autenticación SAML, publicación de aplicaciones institucionales y conexión de usuarios externos.



2. Revisar y fortalecer configuraciones de autenticación SAML:

Validar todos los servicios configurados como **SAML Identity Provider (SAML IdP)**, revisando certificados, configuraciones de confianza, integraciones con proveedores de identidad y aplicaciones dependientes. Se recomienda deshabilitar funcionalidades no utilizadas y aplicar configuraciones seguras que reduzcan la superficie de exposición del dispositivo.

3. Implementar autenticación multifactor (MFA) y controles adicionales de acceso:

Fortalecer los mecanismos de autenticación asociados a NetScaler Gateway mediante MFA, políticas de acceso condicional, validación de dispositivos autorizados y restricciones basadas en ubicación o comportamiento, reduciendo el riesgo de uso indebido de sesiones o credenciales comprometidas.

4. Restringir la exposición de servicios NetScaler hacia internet:

Aplicar controles de segmentación de red, listas de acceso, filtrado de direcciones IP autorizadas y publicación únicamente de servicios necesarios. Evitar la exposición innecesaria de interfaces administrativas y limitar los accesos privilegiados exclusivamente a personal autorizado.

5. Gestionar adecuadamente cuentas administrativas y privilegios:



Revisar periódicamente usuarios administradores, cuentas de servicio y accesos privilegiados asociados al dispositivo. Aplicar principios de mínimo privilegio, eliminar cuentas innecesarias, utilizar credenciales robustas y mantener trazabilidad de todas las actividades administrativas realizadas sobre la plataforma.

6. Monitorear eventos y registros de comportamiento anómalo:

Implementar mecanismos de monitoreo continuo sobre los dispositivos NetScaler para identificar posibles intentos de explotación o accesos sospechosos. Se recomienda:

- Revisar intentos anómalos de autenticación SAML.
- Detectar accesos desde ubicaciones o direcciones IP no habituales.
- Analizar cambios inesperados en configuraciones.
- Identificar creación o modificación no autorizada de usuarios, políticas o servicios publicados.
- Integrar los registros con plataformas SIEM o herramientas de monitoreo institucional.

7. Realizar evaluaciones periódicas de vulnerabilidades y pruebas de seguridad:

Ejecutar análisis de vulnerabilidades, revisiones de configuración y pruebas de seguridad sobre dispositivos NetScaler, incluyendo infraestructura administrada por terceros. Estas



evaluaciones deben permitir identificar versiones obsoletas, configuraciones inseguras, servicios innecesarios o posibles brechas que puedan ser aprovechadas por atacantes.

8. Fortalecer la seguridad de accesos remotos y proveedores externos:

Revisar los accesos proporcionados a usuarios externos, contratistas y proveedores tecnológicos mediante NetScaler Gateway, asegurando controles como accesos temporales, autorización previa, registro de actividades, monitoreo de sesiones y eliminación de permisos cuando finalicen las labores requeridas.

9. Aplicar estrategia de defensa en profundidad:

Garantizar que la infraestructura tecnológica cuente con múltiples capas de protección, incluyendo firewall perimetral, segmentación de redes, sistemas de detección y prevención de intrusiones (IDS/IPS), soluciones EDR/XDR, monitoreo centralizado de eventos y políticas de respuesta ante incidentes. Adicionalmente, promover buenas prácticas de seguridad entre administradores y usuarios para reducir riesgos asociados a vulnerabilidades futuras.

Recomendaciones de respuesta ante compromiso

En caso de que se confirme un compromiso debido a la explotación de la vulnerabilidad **CVE-2026-8451** en dispositivos **Citrix NetScaler ADC o NetScaler Gateway**, las organizaciones del sector salud deben ejecutar acciones inmediatas orientadas a contener



el incidente, reducir el impacto operativo, preservar evidencias y restaurar la seguridad de los servicios de acceso remoto y autenticación afectados.

1. Aislamiento del dispositivo comprometido:

2. Desconectar o restringir temporalmente el acceso del dispositivo NetScaler afectado de la red externa e interna, evitando que un atacante continúe utilizando el componente comprometido como punto de entrada hacia otros sistemas institucionales. En caso de múltiples dispositivos afectados, establecer medidas de contención coordinadas para evitar la propagación del incidente.

2. Aplicación urgente de actualizaciones de seguridad:

Instalar las versiones corregidas publicadas por Citrix para **NetScaler ADC y NetScaler Gateway**, verificando que los dispositivos de producción, contingencia, respaldo y ambientes de prueba queden actualizados. Posteriormente, validar que los servicios publicados funcionen correctamente bajo una configuración segura.

3. Revocación de sesiones y tokens de autenticación:

Realizar la invalidación de sesiones activas, tokens SAML, credenciales temporales y mecanismos de autenticación asociados al dispositivo comprometido. Se recomienda forzar



nuevos procesos de autenticación para usuarios internos, externos y proveedores que hayan utilizado servicios protegidos mediante NetScaler.

4. Auditoría de registros y actividades del dispositivo:

Ejecutar una revisión detallada de los registros generados por NetScaler, sistemas de autenticación, firewalls y herramientas de monitoreo, buscando indicadores asociados a explotación o acceso no autorizado, tales como:

- Solicitudes SAML anómalas.
- Intentos repetitivos de autenticación.
- Accesos administrativos no autorizados.
- Cambios inesperados en configuraciones.
- Conexiones desde direcciones IP o ubicaciones inusuales.
- Creación o modificación no autorizada de políticas y servicios publicados.

5. Restablecimiento de credenciales administrativas y cuentas críticas:

Realizar cambio de contraseñas de cuentas administrativas asociadas al dispositivo y evaluar la necesidad de rotación de credenciales utilizadas en integraciones con otros sistemas. Se debe priorizar cualquier cuenta con privilegios elevados o acceso a plataformas



críticas como historia clínica electrónica, sistemas administrativos o servicios de proveedores.

6. Análisis forense del dispositivo y componentes relacionados:

Realizar un análisis técnico y forense sobre el dispositivo comprometido, conservando evidencias digitales antes de ejecutar acciones que puedan alterar información relevante. El análisis debe incluir revisión de configuraciones, archivos de registro, conexiones establecidas, usuarios activos, cambios recientes y posibles indicadores de persistencia.

7. Revisión de sistemas conectados y posibles movimientos laterales:

Evaluar los sistemas que dependan del acceso proporcionado por NetScaler Gateway, incluyendo aplicaciones clínicas, servidores internos, plataformas administrativas, sistemas de laboratorio y servicios utilizados por terceros. Se debe determinar si existieron accesos no autorizados posteriores al compromiso inicial.

8. Restauración desde configuraciones y respaldos seguros:

En caso de detectar alteraciones en la configuración del dispositivo o afectación de servicios, realizar la recuperación utilizando respaldos verificados y libres de compromiso. Toda restauración debe ejecutarse después de aplicar parches de seguridad y validar las condiciones de seguridad del entorno.



9. Notificación y gestión del incidente de seguridad:

Informar inmediatamente al equipo interno de seguridad, CSIRT institucional o responsable de tecnología. Si el incidente involucra exposición de información personal, datos clínicos o información sensible de pacientes, realizar la gestión correspondiente conforme a los procedimientos internos y las obligaciones establecidas en la normativa colombiana de protección de datos personales, incluyendo la **Ley 1581 de 2012** y demás disposiciones aplicables.

10. Comunicación con usuarios, proveedores y partes interesadas:

Cuando exista afectación sobre cuentas de usuarios, accesos remotos o información sensible, establecer comunicaciones claras con las partes involucradas, indicando las medidas adoptadas, acciones requeridas y recomendaciones para proteger los accesos institucionales.

11. Revisión posterior al incidente y fortalecimiento de controles:

Una vez controlada la situación, realizar un análisis de causa raíz para identificar oportunidades de mejora. Se recomienda fortalecer controles como autenticación multifactor (MFA), segmentación de red, monitoreo continuo, gestión de privilegios, revisión



periódica de accesos externos y actualización permanente de dispositivos críticos de seguridad.

Conclusiones

La vulnerabilidad **CVE-2026-8451** representa un riesgo significativo para las organizaciones del sector salud que utilizan dispositivos **Citrix NetScaler ADC y NetScaler Gateway** como mecanismos de acceso remoto, publicación de aplicaciones o gestión de autenticación centralizada. La explotación de esta falla podría permitir a un atacante remoto no autenticado acceder a información almacenada temporalmente en memoria del dispositivo, afectando la confidencialidad de los procesos de autenticación y comprometiendo la seguridad de los servicios tecnológicos asociados.

El impacto de esta vulnerabilidad puede extenderse tanto a nivel técnico, afectando la seguridad de los dispositivos perimetrales y mecanismos de control de acceso, como a nivel operativo, generando riesgos sobre la continuidad de servicios esenciales utilizados por instituciones de salud, incluyendo plataformas clínicas, sistemas administrativos, servicios de telemedicina, accesos remotos de profesionales y conexiones con proveedores tecnológicos.

La aplicación inmediata de las actualizaciones de seguridad publicadas por Citrix, junto con la revisión de configuraciones SAML, fortalecimiento de controles de autenticación, monitoreo de registros y análisis preventivo de posibles compromisos, resulta fundamental para reducir la probabilidad de explotación y limitar el impacto de posibles incidentes de seguridad.

Adicionalmente, es indispensable que las organizaciones del sector salud mantengan una gestión continua de vulnerabilidades sobre sus dispositivos críticos de infraestructura,



realizando inventarios tecnológicos actualizados, revisiones periódicas de configuraciones, control de accesos privilegiados y seguimiento permanente de alertas de seguridad emitidas por fabricantes y organismos especializados.

La adopción de estas medidas permitirá a las entidades de salud fortalecer la protección de sus servicios tecnológicos, salvaguardar la información clínica y administrativa de pacientes, garantizar la continuidad operacional y cumplir con los requerimientos de seguridad y protección de datos establecidos en la normativa vigente, consolidando una postura de ciberseguridad preventiva y resiliente frente a nuevas amenazas.

Fuentes:



Citrix Security Bulletin – NetScaler ADC and NetScaler Gateway Security Bulletin for CVE-2026-8451 – Publicación oficial de Citrix con información sobre la vulnerabilidad, productos afectados, versiones vulnerables, condiciones de explotación y actualizaciones de seguridad disponibles.

o URL: <https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696604>

• **National Vulnerability Database (NVD) – CVE-2026-8451** – Base de datos oficial del NIST con información técnica de la vulnerabilidad, clasificación, puntuación CVSS, vector de ataque, referencias y productos afectados.

o URL: <https://nvd.nist.gov/vuln/detail/CVE-2026-8451>

• **Common Vulnerabilities and Exposures (CVE) – MITRE Corporation** – Registro oficial de identificación de la vulnerabilidad CVE-2026-8451, incluyendo descripción técnica y referencias del fabricante.

o URL: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2026-8451>



- **NHS England Digital – Cyber Alert sobre Citrix NetScaler** – Alerta técnica dirigida al sector salud que describe el impacto potencial de la vulnerabilidad, escenarios de riesgo y recomendaciones de mitigación para organizaciones sanitarias.
o URL: <https://digital.nhs.uk/cyber-alerts>
- **INCIBE-CERT – Múltiples vulnerabilidades en NetScaler de Citrix** – Aviso técnico de ciberseguridad con información sobre productos afectados, impacto, versiones corregidas y recomendaciones de actualización.
o URL: <https://www.incibe.es/incibe-cert/alerta-temprana/avisos/multiples-vulnerabilidades-en-netscaler-de-citrix>
- **CISA – Known Exploited Vulnerabilities Catalog (KEV)** – Catálogo oficial de vulnerabilidades explotadas activamente utilizado para priorización de remediación y gestión de riesgos.
o URL: <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- **WatchTowr Labs – Análisis técnico CVE-2026-8451 Citrix NetScaler Memory Overread** – Investigación técnica independiente sobre la vulnerabilidad, comportamiento de explotación y análisis del fallo de lectura de memoria.
o URL: <https://labs.watchtowr.com/citrixbleed-to-infinity-and-beyond-citrix-netscaler-pre-auth-memory-overread-cve-2026-8451/>

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el **CSIRT Salud** a través de las líneas telefónicas **(+57) 316 893 1490 - 318 155 3570** o mediante el correo electrónico **csirtsalud@minsalud.gov.co**. Nuestro equipo está disponible para brindar el acompañamiento necesario.

