

Alerta ID:	130
Fecha del reporte:	05/08/2026
Entidad:	Entidades del ecosistema digital
Título:	Bypass de autenticación y toma de control de cuentas.
Herramienta de detección	N/A
Activo involucrado:	• Firewalls FortiGate • Puertas de enlace VPN • Actividad de actores en la dark web
Tipo de alerta:	Alerta
Nivel de riesgo:	Alto

Objetivo:

Informar a las organizaciones del sector salud en Colombia sobre la identificación de una vulnerabilidad crítica de seguridad en la plataforma N-able N-central, utilizada para administración y monitoreo remoto de infraestructura tecnológica, la cual permite a atacantes remotos evadir mecanismos de autenticación y obtener acceso administrativo no autorizado sobre servidores N-central vulnerables.

El propósito de esta alerta es que las entidades del sector salud validen si cuentan con instalaciones de N-able N-central expuestas o utilizadas dentro de sus ambientes tecnológicos, verifiquen las versiones implementadas, apliquen las actualizaciones de seguridad disponibles y realicen actividades de monitoreo orientadas a identificar accesos administrativos no autorizados, modificaciones en agentes administrados y posibles actividades de persistencia.



La explotación de esta vulnerabilidad representa un riesgo elevado para organizaciones que utilizan herramientas RMM, debido a que estas plataformas poseen capacidades privilegiadas para administrar múltiples equipos, ejecutar acciones remotas y desplegar configuraciones sobre dispositivos administrados, lo que podría afectar la confidencialidad, integridad y disponibilidad de los servicios tecnológicos que soportan la operación asistencial y administrativa.

Descripción:

Se ha identificado la vulnerabilidad **CVE-2026-18577** en la plataforma **N-able N-central**, una solución de administración y monitoreo remoto (RMM, Remote Monitoring and Management) utilizada por proveedores de servicios administrados (MSP) y organizaciones para supervisar, administrar y ejecutar acciones remotas sobre equipos, servidores y dispositivos conectados.

La vulnerabilidad corresponde a un **bypass de autenticación**, clasificada bajo **CWE-288: Authentication Bypass Using an Alternate Path or Channel**, que permite a un atacante remoto evadir los mecanismos normales de autenticación implementados por la plataforma y obtener acceso no autorizado a funciones administrativas del sistema.

El problema está relacionado con una corrección incompleta aplicada previamente para la vulnerabilidad **CVE-2026-18556**, permitiendo que los atacantes continuaran utilizando rutas alternativas de acceso para superar los controles de autenticación establecidos en N-central.

La explotación exitosa de esta vulnerabilidad puede permitir a un atacante acceder a capacidades privilegiadas de administración remota, incluyendo funciones relacionadas con gestión de dispositivos, ejecución de acciones sobre agentes instalados y control de sistemas administrados por la plataforma.



Debido a la naturaleza de N-central como herramienta RMM, el impacto potencial es elevado, ya que una instancia comprometida puede convertirse en un punto central de acceso hacia múltiples equipos administrados dentro de una organización o de varios clientes conectados al mismo entorno.

Para organizaciones del sector salud, esta situación representa un riesgo significativo debido a que las plataformas RMM suelen utilizarse para administrar infraestructura crítica, estaciones de trabajo administrativas, servidores, dispositivos tecnológicos y ambientes que soportan servicios asistenciales. Un atacante con acceso administrativo podría afectar la disponibilidad, confidencialidad e integridad de los sistemas gestionados.

La vulnerabilidad fue reportada como **explotada activamente**, por lo que N-able recomienda actualizar las instalaciones afectadas a las versiones corregidas disponibles y revisar los registros de autenticación y actividad administrativa para identificar posibles accesos no autorizados.

Información técnica:

- **CVE:** CVE-2026-18577
- **Producto afectado:** N-able N-central
- **Tipo:** Authentication Bypass
- **CWE:** CWE-288 – Authentication Bypass Using an Alternate Path or Channel
- **Severidad:** Alta
- **Impacto principal:** Acceso administrativo no autorizado
- **Vector de ataque:** Remoto
- **Requisito de autenticación:** No requerido para la explotación exitosa
- **Estado:** Explotación activa reportada
- **Vulnerabilidad relacionada:** CVE-2026-18556



Riesgo principal para el sector salud:

El compromiso de una plataforma N-central puede permitir a un atacante obtener control sobre herramientas utilizadas para administración remota de infraestructura tecnológica, generando un posible punto de entrada para actividades posteriores como reconocimiento interno, despliegue de herramientas maliciosas, modificación de configuraciones, acceso a equipos administrados o interrupción de servicios tecnológicos críticos.

Consecuencias de la explotación

La explotación exitosa de la vulnerabilidad **CVE-2026-18577** en la plataforma **N-able N-central** puede generar un impacto elevado debido a que esta solución cuenta con capacidades administrativas centralizadas para supervisar, gestionar y ejecutar acciones remotas sobre múltiples dispositivos y sistemas.

A diferencia de una vulnerabilidad que afecta un único equipo, el compromiso de una plataforma RMM puede ampliar el alcance del incidente, ya que el atacante puede utilizar las funciones legítimas de administración para interactuar con los activos tecnológicos gestionados desde la consola comprometida.

1. Acceso administrativo no autorizado a la plataforma N-central

El principal riesgo asociado a esta vulnerabilidad es la evasión de los mecanismos de autenticación, permitiendo que un atacante remoto pueda ingresar a la plataforma sin utilizar los controles normales de validación.

Esto puede permitir:

- Acceso a la consola administrativa de N-central.
- Visualización de organizaciones, clientes o dispositivos administrados.



- Consulta de configuraciones y parámetros del entorno.
- Uso indebido de funciones privilegiadas de administración remota.

Impacto clave:

El atacante puede operar dentro de la plataforma utilizando privilegios administrativos, dificultando la diferenciación entre acciones legítimas y maliciosas.

2. Compromiso de múltiples equipos administrados

Las plataformas RMM tienen la capacidad de administrar numerosos dispositivos desde un punto centralizado. Si un atacante obtiene control sobre N-central, puede aprovechar esta relación de confianza para afectar los equipos conectados.

Los posibles objetivos incluyen:

- Servidores Windows y Linux.
- Estaciones de trabajo administrativas.
- Equipos utilizados por personal asistencial.
- Infraestructura tecnológica gestionada por proveedores externos.
- Dispositivos conectados mediante agentes N-central.

Impacto clave:

Un único punto comprometido puede convertirse en un mecanismo de acceso hacia múltiples activos tecnológicos.

3. Ejecución de acciones remotas no autorizadas

Una cuenta administrativa comprometida en N-central puede permitir el uso indebido de capacidades legítimas de administración remota.

Entre las acciones potenciales se encuentran:



- Ejecución remota de comandos o tareas administrativas.
- Modificación de configuraciones de equipos administrados.
- Instalación o eliminación de software.
- Alteración de agentes de monitoreo.
- Deshabilitación de controles de seguridad.

Impacto clave:

El atacante puede utilizar herramientas legítimas de administración para realizar actividades maliciosas sin necesidad de introducir mecanismos externos inicialmente.

4. Riesgo para la continuidad operativa del sector salud

Las entidades de salud dependen de una infraestructura tecnológica altamente interconectada para soportar procesos asistenciales y administrativos.

El compromiso de una herramienta RMM podría afectar:

- Servidores de aplicaciones institucionales.
- Equipos administrativos.
- Sistemas de soporte tecnológico.
- Plataformas utilizadas por proveedores tecnológicos.
- Servicios digitales necesarios para la operación diaria.

Impacto clave:

La manipulación de sistemas administrados remotamente podría generar interrupciones, degradación del servicio o indisponibilidad temporal de recursos tecnológicos.

5. Instalación de herramientas maliciosas y persistencia

Un atacante con acceso administrativo puede utilizar la plataforma comprometida para desplegar software no autorizado sobre equipos administrados.



Las acciones potenciales incluyen:

- Instalación de herramientas de acceso remoto adicionales.
- Despliegue de malware.
- Creación de mecanismos de persistencia.
- Modificación de configuraciones de seguridad.
- Preparación del entorno para ataques posteriores.

Impacto clave:

La plataforma RMM puede convertirse en un mecanismo legítimo utilizado para distribuir actividades maliciosas dentro del entorno administrado.

6. Exposición de información técnica y operativa

El acceso a N-central puede proporcionar información relevante sobre la infraestructura administrada.

El atacante podría obtener:

- Inventario de dispositivos.
- Sistemas operativos instalados.
- Versiones de software.
- Direcciones IP internas.
- Estado de agentes y servicios.
- Información de configuración.

Impacto clave:

La información obtenida puede facilitar ataques posteriores contra sistemas internos o externos.

7. Compromiso de proveedores tecnológicos y clientes asociados



Muchas organizaciones utilizan plataformas RMM mediante proveedores de servicios administrados (MSP). En estos escenarios, un compromiso de N-central puede tener efectos más amplios.

El riesgo puede extenderse hacia:

- Varias entidades administradas por un mismo proveedor.
- Ambientes tecnológicos compartidos.
- Organizaciones tercerizadas con relaciones de confianza.

Impacto clave:

La afectación puede propagarse a través de relaciones tecnológicas existentes entre proveedores y entidades de salud.

8. Riesgo de acceso a sistemas críticos del sector salud

Aunque la vulnerabilidad no compromete directamente sistemas clínicos específicos, el acceso administrativo a la plataforma de gestión puede facilitar actividades posteriores contra activos conectados.

El riesgo potencial incluye:

- Acceso indirecto a servidores institucionales.
- Compromiso de estaciones de trabajo.
- Afectación de servicios tecnológicos de soporte asistencial.
- Exposición de información almacenada en equipos administrados.

Impacto clave:

La gravedad dependerá del alcance de administración otorgado a la instancia N-central y de los controles adicionales implementados por la organización.



9. Impacto regulatorio y reputacional

Si la explotación deriva en acceso no autorizado, modificación de sistemas o exposición de información, la organización puede enfrentar consecuencias regulatorias.

Los posibles impactos incluyen:

- Investigación interna y análisis forense.
- Evaluación de afectación de datos personales.
- Notificación a autoridades cuando corresponda.
- Requerimientos de entidades regulatorias.
- Pérdida de confianza institucional.

En Colombia, las entidades responsables del tratamiento de información deben aplicar medidas de seguridad adecuadas conforme al régimen de protección de datos personales establecido en la Ley 1581 de 2012.

Impacto clave:

El incidente puede generar consecuencias técnicas, operativas, legales y reputacionales para la institución afectada.

Modo de explotación del ataque



La explotación de la vulnerabilidad **CVE-2026-18577** en **N-able N-central** se basa en un mecanismo de **evasión de autenticación**, mediante el cual un atacante remoto puede acceder a funciones administrativas de la plataforma sin completar los controles normales de autenticación.

Debido a que N-central es una plataforma de administración remota con privilegios elevados, la explotación permite al atacante obtener una posición de control sobre la consola de gestión



y utilizar las capacidades legítimas de administración para interactuar con los dispositivos registrados.

La cadena de ataque puede desarrollarse de la siguiente manera:

FASE 1 – IDENTIFICACIÓN DEL OBJETIVO

El atacante inicia con actividades de reconocimiento orientadas a identificar organizaciones que utilizan instalaciones de **N-able N-central** expuestas o accesibles desde internet.

Las actividades pueden incluir:

- Identificación de servidores N-central accesibles públicamente.
- Reconocimiento de dominios asociados a organizaciones objetivo.
- Identificación de proveedores de servicios administrados (MSP) que utilizan N-central.
- Análisis de infraestructura tecnológica expuesta.

El objetivo es localizar plataformas RMM que puedan ser utilizadas como punto de acceso privilegiado.

MITRE ATT&CK:

- T1595 – Active Scanning.
- T1580 – Cloud Infrastructure Discovery.

FASE 2 – EXPLOTACIÓN DEL BYPASS DE AUTENTICACIÓN

El atacante envía solicitudes especialmente construidas hacia la instancia vulnerable de N-central con el objetivo de evadir los mecanismos normales de autenticación.

La vulnerabilidad **CVE-2026-18577** permite utilizar una ruta alternativa de acceso que evita la validación esperada de identidad.

La explotación aprovecha:

- Debilidades en los controles de autenticación.
- Validaciones insuficientes de acceso.



- Rutas alternativas dentro de la aplicación.
- Fallas en la implementación del mecanismo de autenticación.

CWE asociado:

- CWE-288 – Authentication Bypass Using an Alternate Path or Channel.

MITRE ATT&CK:

- T1190 – Exploit Public-Facing Application.

FASE 3 – ACCESO A LA CONSOLA ADMINISTRATIVA

Una vez explotada la vulnerabilidad, el atacante puede obtener acceso no autorizado a la interfaz administrativa de N-central.

Desde la consola comprometida puede realizar acciones como:

- Visualizar dispositivos administrados.
- Consultar información del entorno.
- Acceder a configuraciones administrativas.
- Interactuar con agentes instalados.
- Utilizar funciones remotas disponibles en la plataforma.

Riesgo clave:

El atacante obtiene capacidades similares a las de un administrador legítimo de la plataforma.

MITRE ATT&CK:

- T1078 – Valid Accounts (si posteriormente utiliza cuentas válidas).
- T1219 – Remote Access Software.

FASE 4 – RECONOCIMIENTO DEL ENTORNO ADMINISTRADO

Después de obtener acceso a N-central, el atacante puede realizar reconocimiento sobre los activos gestionados.



Puede identificar:

- Equipos registrados.
- Sistemas operativos.
- Versiones de software.
- Agentes instalados.
- Grupos de dispositivos.
- Infraestructura administrada por la organización.

Esta información permite determinar cuáles activos tienen mayor valor estratégico.

MITRE ATT&CK:

- T1018 – Remote System Discovery.
- T1087 – Account Discovery.
- T1518 – Software Discovery.

FASE 5 – ABUSO DE FUNCIONES DE ADMINISTRACIÓN REMOTA

Al controlar la plataforma RMM, el atacante puede aprovechar funciones legítimas para ejecutar acciones sobre los equipos administrados.

Las capacidades potencialmente abusables incluyen:

- Ejecución remota de comandos.
- Despliegue de software.
- Modificación de configuraciones.
- Gestión de agentes.
- Ejecución de tareas programadas.

Estas acciones pueden realizarse utilizando herramientas propias de la plataforma, reduciendo la necesidad de instalar mecanismos externos inicialmente.

MITRE ATT&CK:



- T1569.002 – System Services: Service Execution.
- T1059 – Command and Scripting Interpreter.

FASE 6 – PERSISTENCIA EN EL ENTORNO

Después del acceso inicial, el atacante puede intentar mantener presencia dentro del entorno comprometido.

Las acciones potenciales incluyen:

- Creación o modificación de cuentas administrativas.
- Instalación de herramientas adicionales de acceso remoto.
- Alteración de configuraciones de administración.
- Uso de agentes existentes como mecanismo de permanencia.

MITRE ATT&CK:

- T1098 – Account Manipulation.
- T1543 – Create or Modify System Process.

FASE 7 – MOVIMIENTO HACIA ACTIVOS ADMINISTRADOS

Una plataforma RMM comprometida puede convertirse en un punto de distribución hacia múltiples equipos conectados.

El atacante podría intentar:

- Acceder a servidores administrados.
- Comprometer estaciones de trabajo.
- Buscar credenciales almacenadas.
- Expandir el acceso hacia otros sistemas internos.

El alcance dependerá de:

- Permisos asignados en N-central.
- Cantidad de dispositivos administrados.



- Segmentación de red existente.
- Controles adicionales implementados.

MITRE ATT&CK:

- T1021 – Remote Services.
- T1078 – Valid Accounts.

FASE 8 – IMPACTO FINAL

Con control sobre la plataforma administrativa, un atacante podría ejecutar acciones orientadas a:

- Robo de información.
- Interrupción de servicios tecnológicos.
- Despliegue de malware o ransomware.
- Modificación de configuraciones críticas.
- Compromiso de múltiples equipos administrados.

En organizaciones del sector salud, el impacto puede extenderse a sistemas tecnológicos que soportan procesos asistenciales y administrativos.

MITRE ATT&CK:

- T1486 – Data Encrypted for Impact.
- T1490 – Inhibit System Recovery.
- T1565 – Data Manipulation.

Recomendaciones de detección y mitigación

Para reducir el riesgo asociado a la vulnerabilidad **CVE-2026-18577** en **N-able N-central**, las organizaciones del sector salud deben implementar controles orientados a la protección de plataformas de administración remota, fortalecimiento del acceso administrativo, monitoreo continuo y validación de actividades realizadas sobre los dispositivos gestionados.



Debido a que las herramientas RMM poseen privilegios elevados sobre múltiples activos tecnológicos, deben ser tratadas como sistemas críticos dentro de la arquitectura de seguridad institucional.

DETECCIÓN EN SIEM / SOC (MONITOREO AVANZADO)

Detección de accesos administrativos anómalos

Configurar alertas para identificar:

- Accesos a la consola N-central desde direcciones IP no habituales.
- Inicios de sesión administrativos desde países o ubicaciones no esperadas.
- Múltiples intentos fallidos de autenticación seguidos de acceso exitoso.
- Accesos fuera del horario operativo normal.
- Uso de cuentas administrativas desde dispositivos no reconocidos.
- Cambios repentinos en patrones de administración.

MITRE ATT&CK:

- T1078 – Valid Accounts.
- T1098 – Account Manipulation.

Objetivo:

Identificar posibles accesos no autorizados a la plataforma de administración remota.

Monitoreo de actividad administrativa en N-central

Supervisar:



- Creación o modificación de cuentas administrativas.
- Cambios en permisos y roles.
- Modificación de políticas de administración.
- Ejecución de comandos remotos no autorizados.
- Instalación de software mediante la consola.
- Cambios masivos sobre grupos de dispositivos.

Indicadores de riesgo:

- Actividades administrativas realizadas por usuarios que normalmente no ejecutan estas funciones.
- Cambios simultáneos sobre múltiples equipos.
- Acciones realizadas inmediatamente después de un acceso sospechoso.

MITRE ATT&CK:

- T1059 – Command and Scripting Interpreter.
- T1569.002 – System Services: Service Execution.

DETECCIÓN DE ACTIVIDAD SOBRE EQUIPOS ADMINISTRADOS

Monitorear los dispositivos gestionados por N-central:

- Ejecución de procesos nuevos después de tareas remotas.
- Instalación inesperada de aplicaciones.
- Cambios en servicios del sistema.
- Creación de usuarios locales.
- Modificaciones en configuraciones de seguridad.
- Conexiones remotas no habituales.



Objetivo:

Identificar posibles acciones posteriores realizadas mediante la plataforma comprometida.

MITRE ATT&CK:

- T1543 – Create or Modify System Process.
- T1053 – Scheduled Task/Job.

RESTRICCIÓN DE EXPOSICIÓN DE LA PLATAFORMA RMM

Aplicar controles de acceso:

- Evitar exposición directa de N-central hacia internet cuando no sea estrictamente necesario.
- Restringir acceso administrativo mediante VPN corporativa o redes autorizadas.
- Implementar listas de control de acceso por IP.
- Limitar accesos administrativos únicamente a personal autorizado.
- Separar la administración RMM de redes operativas y asistenciales.

Objetivo:

Reducir la superficie de ataque disponible para explotación remota.

ACTUALIZACIÓN Y GESTIÓN DE PARCHES

Acciones prioritarias:

- Actualizar N-able N-central a la versión corregida disponible.
- Validar que todas las instancias administradas se encuentren en versiones soportadas.



- Revisar si existen equipos expuestos antes de aplicar la actualización.
- Mantener un inventario actualizado de plataformas RMM utilizadas por la organización.

Objetivo:

Eliminar la condición vulnerable que permite el bypass de autenticación.

FORTALECIMIENTO DE AUTENTICACIÓN Y PRIVILEGIOS

Implementar:

- MFA obligatorio para cuentas administrativas de N-central.
- Cuentas administrativas individuales, evitando usuarios compartidos.
- Principio de mínimo privilegio.
- Revisión periódica de usuarios y roles asignados.
- Deshabilitación de cuentas administrativas sin uso.
- Rotación de credenciales administrativas.

MITRE ATT&CK:

- T1078 – Valid Accounts.

SEGMENTACIÓN Y CONTROL DE ACCESO

Recomendaciones:

- Ubicar servidores RMM en segmentos protegidos de red.
- Separar redes administrativas de redes clínicas y asistenciales.
- Restringir comunicación entre N-central y activos administrados únicamente a los puertos



requeridos.

- Implementar controles Zero Trust para accesos administrativos.

Objetivo:

Reducir la posibilidad de propagación en caso de compromiso.

PROTECCIÓN DE ENDPOINTS ADMINISTRADOS

En equipos gestionados mediante N-central:

- Mantener EDR/XDR habilitado.
- Supervisar ejecución de herramientas remotas no autorizadas.
- Bloquear instalación de software no aprobado.
- Habilitar registros avanzados de eventos.
- Monitorear cambios en servicios críticos.

MITRE ATT&CK:

- T1562 – Impair Defenses.
- T1543 – Create or Modify System Process.

INTELIGENCIA DE AMENAZAS Y BLOQUEO PROACTIVO

Implementar:

- Integración de indicadores de compromiso asociados a explotación de N-central.
- Monitoreo de direcciones IP sospechosas.
- Revisión de dominios utilizados durante actividades maliciosas.
- Correlación de eventos con campañas activas contra herramientas RMM.



Objetivo:

Detectar intentos de explotación antes de la materialización del incidente.

RECOMENDACIONES DE RESPUESTA ANTE POSIBLE COMPROMISO

Contención inmediata

En caso de identificar explotación:

- Restringir temporalmente el acceso administrativo a N-central.
- Aislar la instancia afectada.
- Bloquear accesos sospechosos.
- Deshabilitar cuentas administrativas comprometidas.
- Revocar sesiones activas.
- Detener tareas remotas no autorizadas.

Objetivo:

Evitar que el atacante continúe utilizando la plataforma como punto de control.

Preservación de evidencia

Recolectar:

- Logs de autenticación de N-central.
- Registros de actividad administrativa.
- Historial de comandos ejecutados.
- Cambios de configuración.
- Inventario de dispositivos administrados.
- Registros de firewall y acceso remoto.



Objetivo:

Determinar el alcance real del compromiso.

Análisis del impacto

Validar:

- Si hubo acceso administrativo no autorizado.
- Equipos afectados mediante la plataforma.
- Comandos o tareas ejecutadas.
- Software instalado posteriormente.
- Cambios realizados en dispositivos administrados.
- Posible exposición de información.

MITRE ATT&CK:

- T1190 – Exploit Public-Facing Application.
- T1078 – Valid Accounts.

Recuperación

Realizar:

- Aplicación del parche de seguridad.
- Restablecimiento de credenciales administrativas.
- Revisión de permisos asignados.
- Eliminación de accesos no autorizados.
- Validación de integridad de equipos administrados.
- Monitoreo reforzado posterior al incidente.



Recomendaciones de respuesta ante compromiso

En caso de sospecha o confirmación de explotación de la vulnerabilidad **CVE-2026-18577** en una instancia de **N-able N-central**, la organización debe activar inmediatamente su plan de respuesta a incidentes, considerando que una plataforma RMM comprometida puede convertirse en un punto de control privilegiado sobre múltiples activos tecnológicos administrados.

La respuesta debe orientarse a contener el acceso del atacante, preservar evidencia, determinar el alcance del compromiso, eliminar mecanismos de persistencia y recuperar la operación bajo condiciones seguras.

CONTENCIÓN INMEDIATA

Las primeras acciones deben estar dirigidas a impedir que el atacante continúe utilizando la plataforma comprometida.

Acciones recomendadas:

- Restringir temporalmente el acceso administrativo a N-central.
- Limitar la exposición externa de la plataforma mientras se realiza la investigación.
- Bloquear direcciones IP asociadas a actividad sospechosa.
- Deshabilitar cuentas administrativas comprometidas o no reconocidas.
- Revocar sesiones activas de usuarios administrativos.
- Suspender temporalmente tareas remotas sospechosas ejecutadas desde la consola.
- Aislar equipos administrados que presenten actividad anómala.

Objetivo:

Interrumpir la capacidad del atacante para continuar utilizando N-central como mecanismo de administración sobre la infraestructura tecnológica.



PRESERVACIÓN DE EVIDENCIA

Antes de realizar cambios que puedan modificar la información disponible, se debe conservar evidencia técnica para el análisis forense.

Recolectar:

- Registros de autenticación de N-central.
- Historial de accesos administrativos.
- Registros de cambios de configuración.
- Actividad de usuarios y roles administrativos.
- Historial de tareas ejecutadas remotamente.
- Inventario de dispositivos gestionados.
- Logs de firewall, VPN y sistemas de monitoreo relacionados.
- Registros de los endpoints administrados.

Validar especialmente:

- Primer acceso sospechoso identificado.
- Usuarios utilizados durante la actividad anómala.
- Equipos afectados por acciones remotas.
- Cambios realizados dentro de la plataforma.

Objetivo:

Garantizar trazabilidad del incidente y determinar la magnitud real del compromiso.

ANÁLISIS Y VALIDACIÓN DEL COMPROMISO

Realizar una investigación detallada para establecer si la explotación fue exitosa y qué acciones realizó el atacante.

Validar:

- Si existieron accesos administrativos no autorizados.
- Si fueron modificados usuarios, roles o permisos.



- Si se crearon cuentas nuevas.
- Si fueron ejecutadas tareas remotas no autorizadas.
- Si hubo instalación de software desconocido.
- Si se modificaron configuraciones de agentes administrados.
- Si otros sistemas fueron alcanzados desde la plataforma.

MITRE ATT&CK:

- T1190 – Exploit Public-Facing Application.
- T1078 – Valid Accounts.
- T1059 – Command and Scripting Interpreter.

ERRADICACIÓN DE LA AMENAZA

Después de determinar el alcance del incidente, se deben eliminar los accesos utilizados por el atacante.

Acciones recomendadas:

- Aplicar la actualización de seguridad correspondiente de N-able N-central.
- Cambiar credenciales administrativas asociadas a la plataforma.
- Eliminar usuarios administrativos no autorizados.
- Revisar y corregir permisos excesivos.
- Revocar accesos remotos no reconocidos.
- Eliminar tareas programadas o scripts no autorizados.
- Validar integridad de agentes instalados en equipos administrados.
- Revisar herramientas adicionales de acceso remoto instaladas.

Objetivo:

Eliminar los mecanismos utilizados para mantener acceso persistente.

RECUPERACIÓN DE SISTEMAS

Una vez contenida la amenaza, realizar la recuperación controlada de los servicios.



Acciones:

- Restaurar el acceso administrativo seguro a N-central.
- Verificar la correcta operación de los agentes administrados.
- Validar la integridad de servidores y estaciones gestionadas.
- Confirmar que no existan modificaciones no autorizadas.
- Reestablecer conexiones administrativas bajo controles reforzados.
- Mantener monitoreo intensivo posterior al incidente.

Para organizaciones del sector salud se debe priorizar la validación de:

- Servidores que soportan aplicaciones críticas.
- Equipos administrativos.
- Infraestructura utilizada por proveedores tecnológicos.
- Sistemas que soportan procesos asistenciales.

ANÁLISIS DE IMPACTO**Determinar:**

- Instancias N-central afectadas.
- Fecha probable de explotación.
- Usuarios administrativos comprometidos.
- Cantidad de dispositivos gestionados expuestos.
- Equipos donde se ejecutaron acciones remotas.
- Información potencialmente comprometida.
- Posibles afectaciones a la continuidad operativa.

Evaluar especialmente si el atacante tuvo capacidad para:

- Ejecutar comandos remotos.
- Instalar software.
- Modificar configuraciones.



- Acceder a sistemas internos.
- Alterar controles de seguridad.

NOTIFICACIÓN Y ESCALAMIENTO

Activar los procedimientos institucionales de gestión de incidentes.

Informar a:

- Equipo CSIRT interno o proveedor de respuesta.
- Centro de Operaciones de Seguridad (SOC).
- Dirección de Tecnología.
- Responsables de infraestructura.
- Área jurídica y cumplimiento.
- Proveedores tecnológicos relacionados.

Si se identifica exposición de información personal o sensible:

- Evaluar obligaciones de notificación conforme al régimen colombiano de protección de datos personales.
- Documentar las acciones tomadas durante la gestión del incidente.

LECCIONES APRENDIDAS Y MEJORA CONTINUA

Después del cierre del incidente:

- Revisar controles de acceso administrativo a plataformas RMM.
- Fortalecer autenticación multifactor en herramientas privilegiadas.
- Reducir exposición pública de consolas administrativas.
- Mejorar reglas de detección en SIEM.
- Actualizar procedimientos de gestión de proveedores tecnológicos.
- Revisar inventario de herramientas RMM utilizadas por la organización.
- Capacitar al personal técnico sobre riesgos asociados a herramientas de administración remota.



Conclusiones



La presente alerta de ciberseguridad evidencia el riesgo asociado al compromiso de plataformas de administración remota (RMM), particularmente **N-able N-central**, debido a la vulnerabilidad **CVE-2026-18577**, la cual permite evadir mecanismos de autenticación y obtener acceso no autorizado sobre una herramienta con capacidades administrativas privilegiadas.

El análisis realizado permite concluir que el impacto de esta vulnerabilidad no se limita al compromiso de una aplicación individual, sino que puede afectar múltiples activos tecnológicos debido a la naturaleza centralizada de las soluciones RMM. Una plataforma de este tipo funciona como un punto de gestión sobre servidores, estaciones de trabajo y dispositivos administrados, por lo que su compromiso puede ampliar significativamente la superficie de afectación dentro de una organización.

Para el sector salud, el riesgo es especialmente relevante debido a la dependencia tecnológica de los servicios asistenciales y administrativos. Un atacante con acceso a una plataforma de administración remota podría utilizar las funciones legítimas del sistema para ejecutar acciones sobre equipos gestionados, modificar configuraciones, desplegar herramientas no autorizadas o afectar la disponibilidad de servicios tecnológicos críticos.

La explotación de CVE-2026-18577 demuestra la importancia de considerar las herramientas RMM como activos críticos dentro de la arquitectura de seguridad institucional, aplicando controles equivalentes a los utilizados para sistemas sensibles como servidores de identidad, plataformas administrativas y servicios esenciales.

Asimismo, se identifica que factores como la exposición innecesaria de consolas administrativas a internet, la falta de actualización de plataformas críticas, controles débiles



sobre cuentas privilegiadas y ausencia de monitoreo continuo incrementan la probabilidad de explotación exitosa.

La mitigación efectiva requiere una estrategia integral basada en gestión de vulnerabilidades, reducción de superficie de ataque, fortalecimiento de identidades administrativas, autenticación multifactor, segmentación de redes, monitoreo de actividad privilegiada y respuesta oportuna ante comportamientos anómalos.

Finalmente, se recomienda a las organizaciones del sector salud verificar inmediatamente la presencia de instancias N-able N-central dentro de sus ambientes tecnológicos, aplicar las actualizaciones de seguridad disponibles, revisar los registros de acceso administrativo y mantener una supervisión permanente sobre las acciones ejecutadas mediante plataformas de administración remota.

La protección de estas herramientas debe ser considerada un elemento prioritario de la ciberseguridad institucional, debido a que un único compromiso puede afectar múltiples sistemas y comprometer la continuidad operativa, confidencialidad e integridad de los servicios tecnológicos que soportan la atención en salud.

Fuentes:



N-able Security Advisories – N-central Security Updates

Publicaciones oficiales de N-able relacionadas con vulnerabilidades de seguridad, actualizaciones, versiones corregidas y recomendaciones para proteger instalaciones de N-central.

o <https://www.n-able.com/security>



National Vulnerability Database (NVD) – CVE-2026-18577

Base de datos oficial del National Institute of Standards and Technology (NIST) utilizada para consultar información técnica de la vulnerabilidad, clasificación, severidad, CWE asociado y referencias de seguridad.
o <https://nvd.nist.gov/>

N-able N-central Documentation and Release Notes

Documentación oficial sobre versiones soportadas, procesos de actualización, administración segura y características de la plataforma N-central.
o <https://documentation.n-able.com/>

MITRE ATT&CK Framework – Enterprise Techniques

Base de conocimiento utilizada para la clasificación de técnicas asociadas a la explotación de aplicaciones expuestas, acceso remoto, abuso de cuentas válidas y ejecución de acciones administrativas. <https://attack.mitre.org/>

MITRE CWE – CWE-288 Authentication Bypass Using an Alternate Path or Channel

Catálogo oficial de debilidades comunes de software utilizado para clasificar vulnerabilidades relacionadas con evasión de mecanismos de autenticación.
o <https://cwe.mitre.org/>

CISA Cybersecurity Advisories

Publicaciones oficiales sobre vulnerabilidades explotadas activamente, recomendaciones de mitigación y protección para organizaciones críticas.
o <https://www.cisa.gov/news-events/cybersecurity-advisories>

CISA Known Exploited Vulnerabilities Catalog (KEV)

Catálogo oficial de vulnerabilidades explotadas en escenarios reales, utilizado como referencia para priorización de remediación en organizaciones críticas.
o <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>



ENISA Threat Landscape (ETL)

Informes de inteligencia sobre amenazas que afectan sectores críticos, incluyendo riesgos asociados a herramientas de administración remota, compromiso de infraestructura y continuidad operativa.

o <https://www.enisa.europa.eu/publications>

Health Sector Cybersecurity Coordination Center (HC3) – Health Sector Cybersecurity Guidance

Publicaciones de ciberseguridad orientadas al sector salud, incluyendo gestión de vulnerabilidades, protección de infraestructura tecnológica crítica y respuesta ante incidentes.

o <https://www.hhs.gov/about/agencies/asha/onc/cybersecurity/index.html>

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.

