Boletín de alerta

Boletín Nro.: 13
Fecha de publicación: 11/02/2026
Tema: Alerta 2026-13 Vulnerabilidad Critica de RCE en BeyondTrust
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

BeyondTrust Remote Support (RS)

- Versiones **25.3.1 y anteriores**.

BeyondTrust Privileged Remote Access (PRA)

- Versiones **24.3.4 y anteriores**.

Descripción

El equipo de BeyondTrust identificó la vulnerabilidad **CVE-2026-1731**, clasificada con una severidad **crítica** de **Ejecución Remota de Código (Remote Code Execution, RCE)** que permite a un atacante no autenticado enviar **solicitudes especialmente manipuladas** para provocar la ejecución de **comandos del sistema operativo con el contexto del usuario del sitio** en instancias vulnerables de los productos de soporte remoto de **BeyondTrust**.

BeyondTrust PRA (Privileged Remote Access) y **RS** (Remote Support) son las plataformas vulnerables cuya función es permitir acceso Seguro y controlado a servidores, dispositivos de red y sistemas críticos sin usar VPN tradicional, demás de que ofrecen soporte remoto para IT y mesas de ayuda.

El fabricante ha asignado el **puntaje máximo de riesgo (CVSS 9.9)** dado que el vector de ataque es remoto y sin prerequisitos (sin autenticación, sin interacción), con impacto alto en confidencialidad, integridad y disponibilidad de los sistemas afectados.

Solución:

Parches y actualizaciones

- **Remote Support (RS):** Actualizar a **25.3.2 o posterior**.
- **Privileged Remote Access (PRA):** Actualizar a **25.1.1 o posterior**.

BeyondTrust aplicó automáticamente parches a sus **instancias SaaS** el **2 de febrero 2026**; las instalaciones **on-premise** requieren actualización manual si no están suscritas a actualizaciones automáticas.

Para más información y descarga sobre los parches visita el siguiente link: https://beyondtrustcorp.service-now.com/csm?id=csm_kb_article&sysparm_article=KB0023293

Requisitos previos para aplicar parches

- Instalaciones de RS anteriores a la **21.3** o PRA anteriores a la **22.1** deben **primero actualizarse** a una versión compatible con el parche antes de aplicar la corrección.

Mitigaciones temporales

- restringir el acceso a servicios RS/PRA mediante controles de red (firewall, VPN, listas de permitidos),
- segmentar y monitorear tráfico hacia puertos de administración,
- aumentar la inspección de comandos y eventos anómalos en servidores afectados.

Información adicional:

- https://www.beyondtrust.com/trust-center/security-advisories/bt26-02
- https://www.cve.org/CVERecord?id=CVE-2026-1731
- https://nvd.nist.gov/vuln/detail/CVE-2026-1731