BeyondTrust Patches Critical Authentication Bypass Flaws in Remote Access Software (CVE-2026-40138 and CVE-2026-40139)

Jul 08, 2026

WHITE

View Alert

BeyondTrust has urged customers to patch two critical **Authentication Bypass** vulnerabilities, tracked as **CVE-2026-40138** and **CVE-2026-40139**, affecting its **Remote Support (RS) and Privileged Remote Access (PRA) software**.

While BeyondTrust's cloud customers were secured by April 21, 2026, self-hosted users must manually apply the security rollup or upgrade to version 25.3.3. Shadowserver currently tracks nearly 2,000 exposed online instances.

Additional Info

Analysis

BeyondTrust has issued an urgent warning regarding two critical Authentication Bypass vulnerabilities, tracked as **CVE-2026-40138** and **CVE-2026-40139**, affecting its Remote Support (RS) and Privileged Remote Access (PRA) software.

These flaws allow unauthenticated remote attackers to circumvent access controls and secure elevated, administrative privileges on targeted appliances. Additionally, two high-severity flaws,

tracked as **CVE-2026-40140** and **CVE-2026-40141**, that triggered denial-of-service conditions were addressed.

While BeyondTrust automatically updated its cloud-based customers, nearly 2,000 self-hosted instances remain exposed online, presenting a significant attack surface if left unpatched.

From the health sector security perspective, these vulnerabilities pose an existential threat to patient care operations and data confidentiality. BeyondTrust software is deeply integrated into hospital networks, enabling vendors and IT staff to remotely administer medical devices, electronic health record (EHR) systems, and internal servers. Given that threat actors historically target remote access tools to deploy ransomware, an unauthenticated bypass here allows attackers to move laterally across a hospital network undetected. This could result in critical care disruptions, widespread medical equipment lockout, and catastrophic HIPAA data breaches.

Recommendations

Health-ISAC recommends organizations review and assess their level of risk to these vulnerabilities and implement the following:

- **Apply Security Patches:** Immediately upgrade self-hosted **BeyondTrust RS** and **PRA** software to **version 25.3.3** or **higher**.
- **Restrict Internet Exposure:** Move all remote support and access appliances behind a secure Virtual Private Network (VPN) or firewall to block public internet access.
- **Enforce Zero-Trust Segmentation:** Isolate critical medical devices, patient databases, and electronic health record (EHR) networks from the remote support environment.
- **Audit Access Logs:** Actively review administrative session logs for any anomalous behavior, unauthorized accounts, or unusual connection times.
- **Implement Multi-Factor Authentication (MFA):** Ensure robust MFA is strictly enforced for all internal IT personnel and external third-party vendors.
- **Review Configurations:** Check and harden current authentication settings to ensure no vulnerable, legacy configurations are active.
- **Reviewing the Health Industry Cybersecurity Practices (HICP):** Managing Threats and Protecting Patients Resources.

<hr size=1 width="100%" align=center>

Alert Id	a275c9d5
Category	Vulnerability Bulletins
References	cve beyondtrust cve 1 hhs bleepingcomputer cve 2 cve 3
Tags	CVE-2026-40141, CVE-2026-40140, CVE-2026-40139, CVE-2026-40138, BeyondTrust Privileged Remote Access (PRA), BeyondTrust Remote Support (RS), BeyondTrust, Denial of Service, Authentication Bypass

---

Access the Health-ISAC Threat Intelligence Portal
Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments
Please email us at toc@h-isac.org

Please provide your feedback

Like Dislike

Download the App
Available on iOS, Android and Web

Download on the App Store | Get it on Google Play