Health-ISAC®
Collaborating for Resilience in Health

VULNERABILITY BULLETINS

BeyondTrust Disclosed Critical Flaw in Remote Support Software (CVE-2026-1731)

TLP:WHITE

Feb 11, 2026

On February 6, 2026, BeyondTrust released a security advisory, disclosing a critical pre-authentication Remote Code Execution (RCE) vulnerability tracked as CVE-2026-1731, affecting its Remote Support (RS) and Privileged Remote Access (PRA) products.

Analysis

CVE-2026-1731 is a critical flaw in the BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA) software. The flaw has a CVSS score of 9.9. In the event of successful exploitation, an unauthenticated attacker could execute operating system commands remotely, resulting in full system compromise.

The affected products are as follows:

BeyondTrust Remote Support (RS):

- Versions 25.3.1 and prior are affected by CVE-2026-1731.
- CVE-2026-1731 is fixed in 25.3.2 and later.

BeyondTrust Privileged Remote Access (PRA):

- Versions 24.3.4 and prior are affected by CVE-2026-1731.
- CVE-2026-1731 is fixed in 25.1.1 and later.

BeyondTrust automatically patched SaaS instances of the vulnerable software on February 2, 2026; however, self-hosted customers remain at risk until they apply manual updates.

BeyondTrust has not reported active exploitation of CVE-2026-1731 in the wild. However, these devices are often targeted by both financially motivated and state-aligned threat actors, like the Chinese hacking group Silk Typhoon, which previously exploited BeyondTrust zero-day flaws (CVE-2024-12356 and CVE-2024-12686) to breach the U.S. government and access sensitive data. Health-ISAC recommends that members prioritize patching of this flaw to mitigate the risk of exploitation.

Recommendations

- If you are a self-hosted BeyondTrust customer, manually apply available patches.

- Segment networks and implement strict network access controls.
- Regularly review logs for suspicious activity.
- Review the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients Resources.

Sources

https://www.beyondtrust.com/trust-center/security-advisories/bt26-02

https://www.helpnetsecurity.com/2026/02/09/beyondtrust-remote-access-vulnerability-cve-2026-1731/

https://www.rapid7.com/blog/post/etr-cve-2026-1731-critical-unauthenticated-remote-code-execution-rce-beyondtrust-remote-support-rs-privileged-remote-access-pra/

https://www.bleepingcomputer.com/news/security/beyondtrust-warns-of-critical-rce-flaw-in-remote-support-software/amp/

Incident Date
Feb 10, 2026 (UTC)

Alert ID 3f8969ce

View Alert

Share Feedback

was this helpful? 👍 | 👎

Tags CVE-2026-1731, BeyondTrust Privileged Remote Access (PRA), BeyondTrust Remote Support (RS), BeyondTrust

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

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

Download Health-ISAC's Information Sharing App.

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.