

CISA Advises Immediate Action on BeyondTrust Remote Support Vulnerability



CISA has identified a critical authentication bypass vulnerability in BeyondTrust Remote Support, urging organizations to apply patches and upgrade their systems to mitigate risks.

- A critical vulnerability affects BeyondTrust Remote Support versions 26.2.3 and earlier.
- Patches are available for supported versions; older versions must be upgraded.
- Cyber actors are actively exploiting this vulnerability.
- Organizations should limit external access to their Remote Support appliances.
- Conduct forensic investigations if a compromise is suspected.

Overview

CISA has reported a critical authentication bypass vulnerability in BeyondTrust Remote Support, affecting versions 26.2.3 and earlier. Organizations using these versions are at risk of exploitation by cyber threat actors who can gain unauthorized access and escalate privileges.

Recommended Actions

Organizations with self-hosted Remote Support appliances should take immediate action to patch their systems. The BT26-05-RS patch is available, but those on older versions must first upgrade to a supported version (24.3.1 or later) to apply the patch. It is also crucial to limit external access to only necessary services and restrict administrative access to trusted networks.

In the event of a suspected compromise, organizations should conduct thorough network and memory forensics to gather evidence. This includes isolating any compromised appliances and collecting relevant logs for analysis. Following a forensic investigation, organizations should rebuild their systems from a known-good state, apply the necessary patches, and rotate all stored credentials to enhance security.

What to do now

1. Apply the BT26-05-RS patch immediately if using a supported version.
2. Upgrade to version 24.3.1 or later if on an older version.
3. Limit external access to necessary services only.
4. Restrict administrative access to trusted networks.
5. Conduct forensic investigations if a compromise is suspected.