

FOR IMMEDIATE RELEASE

October 22, 2026

Limehawk Urges BeyondTrust Remote Support Users to Patch After CISA Alert

CISA says attackers are exploiting an authentication bypass in the remote access appliance. Self-hosted appliances need BeyondTrust's patch now.

KNOXVILLE, Tenn., Oct. 22, 2026. Limehawk, LLC, a Knoxville managed IT services provider, today urged businesses that run self-hosted BeyondTrust Remote Support appliances to apply BeyondTrust's BT26-05-RS patch and check for signs of compromise, after CISA warned that the flaw is being exploited.

The vulnerability, CVE-2026-102764, affects Remote Support (formerly Bomgar) versions 26.2.3 and earlier. BeyondTrust says internal components of the product "did not adequately validate the origin of the messages it received," which under the right conditions could let a remote attacker perform file operations on the appliance. CISA calls it a critical authentication bypass. NVD scores it 9.8 under CVSS v3.1, and BeyondTrust rates it 9.3, Critical, under CVSS v4.0. BeyondTrust published its advisory on Oct. 15, 2026.

CISA added the flaw to its Known Exploited Vulnerabilities catalog on Oct. 16. In its alert, CISA said: "Cyber threat actors are actively exploiting the vulnerability to gain initial access, then establishing persistence, escalating privileges, and moving laterally."

BeyondTrust said "a suspected China-nexus espionage actor exploited a zero-day vulnerability," and that the exploitation began on Aug. 29, 2026. BeyondTrust released the patch on Oct. 8 and says its hosted (SaaS) Remote Support customers have already been patched.

Who needs to act?

Any organization that runs its own Remote Support appliance. If an IT provider supports your business remotely, it may run one on your behalf.

BeyondTrust also released the patch for Privileged Remote Access as a precaution. It says internal testing found no way to exploit the flaw in that product, but Privileged Remote Access shares the affected code, and BeyondTrust recommends self-hosted customers apply the patch immediately.

What should businesses do?

Limehawk recommends these steps:

- **Find out if you run it.** Check whether you, or the IT provider that supports you, run a self-hosted BeyondTrust Remote Support or Bomgar appliance.
- **Patch now.** Apply BT26-05-RS on versions 24.3.1 through 26.2.3. Older versions must be upgraded before the patch can be applied. Appliances not subscribed to automatic updates need it applied by hand.
- **Check for compromise.** Exploitation started before a fix existed. CISA recommends network and memory forensics on affected self-hosted appliances. Hunt for unrecognized privileged or administrative sessions, unrecognized script files, unexpected gaps in logs or log forwarding, and unauthorized account, permission or session-policy changes.
- **Restrict exposure.** CISA and BeyondTrust say to limit external access to the services users and customers need, and to restrict administrative interfaces to trusted networks.

- **Get logs off the appliance.** BeyondTrust says the actor deletes local logs and recommends forwarding syslog and session events to a SIEM.

What if the appliance was compromised?

CISA recommends isolating the appliance, taking a snapshot or forensic image, and rebuilding from a known-good state with the BT26-05-RS patch. Then rotate every credential the appliance stored or injected, revoke all active support sessions, and review new multifactor authentication registrations on privileged accounts. BeyondTrust asks customers who find evidence of exploitation to open a Sev 1 support request citing "BT26-05."

Sources

1. BeyondTrust, "Security Advisory BT26-05." Oct. 15, 2026.
<https://www.beyondtrust.com/trust-center/security-advisories/bt26-05>
2. BeyondTrust, "ARMORY CASTLE and BT26-05: What Security Teams Need to Know." Updated Oct. 16, 2026.
<https://www.beyondtrust.com/blog/entry/bt26-05>
3. CISA, "CISA Urges Patching Critical Vulnerability in BeyondTrust Remote Support." Oct. 16, 2026.
<https://www.cisa.gov/news-events/alerts/2026/10/16/cisa-urges-patching-critical-vulnerability-beyondtrust-remote-support>
4. NVD, "CVE-2026-102764." Published Oct. 15, 2026.
<https://nvd.nist.gov/vuln/detail/CVE-2026-102764>

Media Contact

Corey Watson, Managing Member
Limehawk, LLC
press@limehawk.io
<https://limehawk.io>

###