EnCyb

Severity: Critical

Advisory Type: Security

# BeyondTrust Server Compromise via Active RCE Exploitation

Advisory Report

TLP: WHITE

## SECURITY THREAT ADVISORY COUNCIL (STAC)

Empowering organizations with cutting-edge cybersecurity strategies to combat emerging digital threats effectively.

# EXECUTIVE SUMMARY

The Cybersecurity and Infrastructure Security Agency (CISA) have issued a warning that a critical remote code execution (RCE) vulnerability (CVE-2026-1731) in BeyondTrust products is now being actively exploited in ransomware attacks. The flaw allows attackers to remotely execute arbitrary code on vulnerable systems, leading to full compromise.

Threat actors are leveraging this vulnerability as an initial access vector to deploy ransomware, escalate privileges, and move laterally within victim networks. Due to the widespread deployment of BeyondTrust solutions in enterprise and government environments, successful exploitation presents a high-impact risk to affected organizations.

- CVE: CVE-2026-1731
- CVSS: 9.8
- Active Region: Global
- Affected Sector: Multiple sectors
- Affected Product: BeyondTrust Privileged Access Management Solutions
- Severity: Critical
- Published Date: February 21, 2026

# TECHNICAL DETAILS

- **Vulnerability Overview:** The vulnerability enables unauthenticated or low-privileged remote code execution in affected BeyondTrust products.
- **Attack Vector:** The flaw can be exploited remotely over the network if the affected service is exposed. No user interaction is required for successful exploitation.
- **Exploitation in Ransomware Campaigns:** Threat actors are exploiting the flaw to gain initial footholds in target environments. Post-exploitation activity includes credential access, lateral movement, and ransomware deployment.

- **Post-Compromise Capabilities:** Execution of arbitrary commands with elevated privileges. Deployment of backdoors and malware loaders.

## AFFECTED PRODUCTS & VERSION

- BeyondTrust Remote Support: version 25.3.1 and earlier are affected.
- BeyondTrust Privileged Remote Access (PRA): version 24.3.4 and earlier are affected.

## FIXED VERSIONS & REMEDIATION

- For Remote Support, apply version 25.3.2 or later.
- For Privileged Remote Access, upgrade to version 25.1.1 or later.
- Cloud/SaaS instances of both products were automatically patched by the vendor (no manual action required for SaaS).

## IMPACT

- Full compromise of BeyondTrust servers and managed systems.
- Unauthorized remote code execution.
- Increased difficulty in detection and forensic analysis.
- Credential theft and privilege escalation, enabling deployment of additional malware, ransomware, or backdoors.

## RECOMMENDATIONS

- Apply BeyondTrust security patches immediately for all affected versions
- Follow CISA guidance and mitigation recommendations
- Restrict external access to BeyondTrust management interfaces
- Conduct compromise assessments if exposure is suspected
- Isolate affected systems if exploitation indicators are detected

## REFERENCE

- https://www.bleepingcomputer.com/news/security/cisa-beyondtrust-rce-flaw-now-exploited-in-ransomware-attacks/
- https://www.scworld.com/news/cisa-update-beyondtrust-rce-exploited-in-ransomware-attacks

# SECURE, SCALE, SUCCEED WITH

# CONFIDENCE

EnCyb

www.encyb.com/contact-us/ EnCyb soc@encyb.com www.encyb.com