NCA-06.110226 – National CERT Advisory

Critical Pre-Authentication Remote Code Execution Vulnerability in BeyondTrust Remote Support and Privileged Remote Access (CVE-2026-1731)

A critical pre-authentication Remote Code Execution (RCE) vulnerability has been identified in BeyondTrust Remote Support and Privileged Remote Access (PRA) solutions. The vulnerability, tracked as **CVE-2026-1731**, allows unauthenticated remote attackers to execute arbitrary code on affected appliances by sending specially crafted network traffic.

Successful exploitation requires **no valid credentials and no user interaction**, enabling full system compromise of exposed appliances. Given that these products are commonly deployed for privileged access management and remote administrative control, compromise may result in enterprise-wide security impact including credential theft, session hijacking, lateral movement, and persistent backdoor installation.

Immediate patching and validation of system integrity is strongly required, particularly for externally exposed or VPN-accessible appliances.

DOCUMENT SUMMARY

Field	Value
Advisory ID	NCA-02.110226
CVE ID	CVE-2026-1731
Threat Type	Unauthenticated Remote Code Execution
Severity	Critical
Attack Vector	Network (Pre-Authentication)
Authentication Required	No
User Interaction	None
CVSS Score	9.9 (Critical – Complete System Compromise)

AFFECTED PRODUCTS

Product	Affected Versions	Patched Versions
BeyondTrust Remote Support	25.3.1 and prior	Patch BT26-02-RS, 25.3.2 and later
Privileged Remote Access (PRA)	24.3.4 and prior	Patch BT26-02-PRA, 25.1.1 and later

IMPACT ANALYSIS

#	Impact Type	Description
1	Full System Compromise	Remote execution of arbitrary code as system-level process
2	Authentication Bypass	Exploitation without valid credentials
3	Privileged Session Hijacking	Interception or manipulation of active remote sessions
4	Credential Theft	Extraction of stored credentials and session tokens
5	Persistent Malware Installation	Ability to implant backdoors or web shells
6	Lateral Movement	Pivoting into internal enterprise networks
7	Privileged Access Infrastructure Compromise	Undermining core remote access and PAM controls

8	Data Exfiltration	Access to sensitive operational or administrative data
9	Service Disruption	Potential instability or malicious shutdown of appliances
10	Enterprise-Wide Security Breach	Compromise extends beyond appliance into managed systems

THREAT CHARACTERISTICS

Characteristic	Details
Threat Category	Critical Infrastructure Software Vulnerability
Threat Status	Publicly disclosed; under active security scrutiny
Root Cause	Improper handling of crafted network traffic enabling pre-auth code execution
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Exploitation Vector	Direct network access to vulnerable appliance
Exposure Risk	High for internet-facing or VPN-accessible deployments
Affected Systems	BeyondTrust Remote Support and PRA appliances
CWE Classifications	CWE-306 (Missing Authentication), CWE-94 (Code Injection), CWE-284 (Improper Access Control), CWE-269 (Improper Privilege Management)

INDICATORS OF COMPROMISE (IoCs)

Category	Indicator	Description	Action
Network	Unusual inbound traffic to appliance management ports	Exploitation attempts	Inspect logs and block source
Logs	Unexpected process spawns tied to remote handlers	Possible code execution	Forensic investigation
System	New or unknown administrative accounts	Persistence mechanism	Immediate credential reset
Configuration	Unauthorized configuration changes	Post-exploitation activity	Restore from trusted backup
File System	Unknown binaries or web shells	Malware implantation	Isolate appliance
Sessions	Suspicious or unexplained privileged sessions	Session hijacking	Review session logs
Traffic	Lateral connections from appliance to internal hosts	Pivoting attempt	Segment and analyze
Monitoring	IDS/IPS alerts referencing CVE-2026-1731	Active scanning or exploitation	Block and escalate
Authentication	Token irregularities	Credential theft indicator	Rotate credentials
Audit	Log tampering or deletion	Anti-forensics activity	Immediate escalation

REMEDIATION ACTIONS

Action Category	Specific Actions	Priority

Immediate Patching	Apply BT26-02-RS (Remote Support) and BT26-02-PRA (PRA); Upgrade to fixed versions	**MANDATORY**
Exposure Reduction	Restrict management interfaces via firewall or IP allowlists	HIGH
Isolation	Remove externally exposed appliances from internet access if unpatched	MANDATORY
Credential Hygiene	Rotate administrative credentials and session tokens post-patch	HIGH
Integrity Review	Conduct forensic review for signs of pre-patch compromise	HIGH
Monitoring	Enable enhanced logging and anomaly detection	REQUIRED
Network Segmentation	Limit appliance connectivity to only required internal systems	HIGH

ACTION SUMMARY & RESPONSE PRIORITIES

Action Type	Specific Steps	Priority	Timeframe
Patching	Apply vendor security updates	MANDATORY	Immediate
Exposure Control	Restrict internet-facing access	HIGH	Immediate
Verification	Validate appliance integrity	HIGH	Within 48 hours
Monitoring	Deploy exploitation detection rules	REQUIRED	Immediate
Credential Reset	Rotate privileged credentials	HIGH	Post-patch
Audit	Review logs for pre-remediation compromise	REQUIRED	Ongoing

MONITORING & DETECTION REQUIREMENTS

#	Control Area	Requirement	Objective
1	Network Monitoring	Monitor inbound traffic to BeyondTrust appliance management ports	Detect unauthorized or suspicious access attempts
2	Host Monitoring	Alert on abnormal process execution within appliance environment	Identify potential exploitation or malicious activity
3	Log Correlation	Correlate authentication logs with unusual session activity	Detect compromised accounts or session hijacking
4	Network Monitoring	Review outbound connections from appliance to internal systems	Identify lateral movement or command-and-control activity
5	IDS/IPS	Monitor IDS/IPS signatures related to CVE-2026-1731	Detect exploitation attempts targeting the specific vulnerability
6	File Integrity Monitoring	Validate file integrity of appliance binaries and configuration	Detect unauthorized modification or persistence mechanisms

MITIGATION (IF PATCHING IS NOT IMMEDIATELY POSSIBLE)

#	Mitigation Control	Description	Risk Reduction Goal
1	Network Segmentation	Restrict access to management interfaces using firewalls and VPN segmentation	Limit exposure to trusted networks only
2	IP Allowlisting	Apply strict IP allowlisting	Prevent unauthorized access from unknown sources

3	Isolation	Disable or isolate affected appliances from untrusted networks	Reduce attack surface and prevent exploitation
4	Enhanced Monitoring	Increase logging verbosity and active monitoring	Improve detection capability during exposure window
5	Incident Response Posture	Treat exposed appliances as potentially compromised	Enable proactive containment and forensic readiness

Note: Mitigation steps reduce exposure but do not eliminate risk. Vendor patching is the only complete remediation.

REFERENCES

Source	URL
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-1731
CVE Record	https://www.cve.org/CVERecord?id=CVE-2026-1731
Tenable	https://www.tenable.com/cve/CVE-2026-1731

CALL TO ACTION – KEY IMPERATIVES

#	Requirement
1	Immediately identify all BeyondTrust Remote Support and PRA deployments
2	Apply vendor patches without delay
3	Prioritize remediation of externally exposed appliances
4	Conduct post-patch forensic integrity review
5	Rotate privileged credentials associated with affected systems
6	Restrict management interface exposure
7	Enhance monitoring for exploitation attempts
8	Assume potential compromise if patching was delayed

WARNING: Failure to immediately remediate CVE-2026-1731 may result in full appliance compromise, credential theft, lateral movement into internal networks, and enterprise-wide security breach. Immediate action is mandatory.