INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-07-07 16:14 UTC

BeyondTrust Patches Critical Auth Bypass Vulnerabilities in Remote Support and Privileged Remote Access

SECURITY ANALYSIS | CRITICAL | CVSS 9.1

SCC Item ID	SCC-STY-2026-0329
Type	Security Analysis
Severity	CRITICAL
CVSS Base Score	9.1
Affected Products	BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA), specific versions not confirmed from available source data
Published	13 hours ago
Discovery Source	Serper

Executive Summary

BeyondTrust has patched four vulnerabilities in its Remote Support (RS) and Privileged Remote Access (PRA) appliance products, including two pre-authentication flaws that can bypass appliance access controls without valid credentials. Organizations using these products for privileged remote access management are at risk of unauthorized access to their privileged access infrastructure. Immediate patching is warranted given the critical CVSS score of 9.1 and the sensitivity of the systems these products protect.

Technical Analysis

BeyondTrust disclosed four vulnerabilities in its Remote Support (RS) and Privileged Remote Access (PRA) appliance products under advisory BT26-02. Two of the four flaws are pre-authentication bypass vulnerabilities (CWE-306: Missing Authentication for Critical Function; CWE-287: Improper Authentication), meaning an unauthenticated remote attacker could bypass appliance access controls under specific conditions without supplying valid credentials. MITRE ATT&CK techniques T1133 (External Remote Services) and T1190 (Exploit Public-Facing Application) are applicable. The vendor-reported CVSS base score is 9.1 (Critical). Specific CVE identifiers, CVSS vectors, EPSS scores, and affected version ranges were not available in the source material provided; consult advisory BT26-02 at the BeyondTrust Trust Center and corresponding NVD entries for authoritative version-level detail and scoring. No confirmed threat actor attribution appears in the available source data. Patches were released by BeyondTrust concurrent with advisory publication.

Action Checklist

1. Step 1: Containment, Identify all instances of BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA) appliances in your environment. If internet-facing instances cannot be patched immediately, restrict external access at the network perimeter or via WAF/IPS rules until the patch is applied. Consult BeyondTrust advisory BT26-02 (https://www.beyondtrust.com/trust-center/security-advisories/bt26-02) for interim workaround guidance.
2. Step 2: Detection, Review appliance access logs for unauthenticated or anomalous session activity prior to patch application, focusing on MITRE T1133 (External Remote Services) and T1190 (Exploit Public-Facing Application) patterns. Look for access attempts that bypassed normal authentication flows, unexpected session initiations from unknown IPs, and any privilege escalation events on systems managed through these appliances. Correlate with firewall and proxy logs for external access to appliance management ports. Enable audit logging per NIST AU-2 and AU-12 if not already active.
3. Step 3: Eradication, Apply the patches specified in BeyondTrust advisory BT26-02. Specific patch identifiers and version upgrade paths should be sourced directly from the advisory, as version-level details were not available in the source data provided. After patching, rotate credentials for all accounts that had access to the affected appliances, consistent with D3-CRO (Credential Rotation), given the possibility that pre-auth bypass may have permitted unauthorized session establishment.
4. Step 4: Recovery, After patching, verify appliance version numbers against BT26-02 remediated version requirements. Confirm authentication controls are functioning correctly by testing unauthenticated access attempts in a controlled manner. Monitor appliance logs for any continued anomalous activity for at least 30 days post-remediation per AU-6 (Audit Record Review, Analysis, and Reporting). Validate that no unauthorized accounts or sessions persist on managed endpoints.
5. Step 5: Post-Incident, Conduct a review of privileged remote access architecture. Assess whether BeyondTrust appliances are segmented from direct internet exposure and require MFA for all administrative access per CIS 6.5 and D3-MFA. Review account inventory per CIS 5.1 and enforce least privilege per NIST AC-6. Document lessons learned and update the vulnerability management process per CIS 7.1 to include faster patching SLAs for pre-authentication critical vulnerabilities in privileged access tooling.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO, legal, and external IR retainer immediately if BeyondTrust appliance logs show any session established without a valid authentication event, or if managed endpoint accounts or configurations were modified during the exposure window, as these conditions indicate active exploitation of the pre-auth bypass and may trigger breach notification obligations under applicable data protection regulations.

Recovery Notes	Post-patch, treat all endpoints managed through the BeyondTrust RS/PRA appliances during the exposure window as potentially compromised until account inventories and privilege assignments have been audited and confirmed clean. Monitor BeyondTrust appliance authentication logs and managed endpoint Security Event Logs (Event IDs 4624, 4625, 4648, 4720, 4728) daily for a minimum of 30 days for indicators of persistence established prior to patching. Re-validate MFA enforcement and network segmentation controls at 30 and 90 days post-patch as part of the lessons-learned closure process.
Forensic Artifacts	BeyondTrust RS/PRA appliance web access logs: HTTP requests to authentication and API endpoints showing source IP, URI path, response code, and session token — specifically requests that received a 200 OK or session cookie without a preceding valid credential submission, which would indicate exploitation of the pre-auth bypass described in BT26-02. | BeyondTrust admin console session audit export: Full session history including session creation timestamp, initiating user/account, source IP, and authentication method recorded for each session — null or missing authentication method fields on sessions from external IPs during the exposure window are the primary forensic indicator for this vulnerability class. | Firewall flow logs for TCP connections to appliance management ports (443, 8200, 8443): Captures external IP addresses that established connections to the appliance during the exposure window, enabling attribution and scope determination for how many external actors may have probed or exploited the pre-auth bypass. | Managed endpoint Windows Security Event Log: Event ID 4624 (successful logon), 4648 (explicit credential logon), 4720 (account created), and 4728 (group membership change) from systems that received remote sessions brokered through the compromised BeyondTrust appliances — attacker lateral movement or persistence following a pre-auth bypass would appear in these records on the destination endpoint rather than the appliance itself. | OS-level user and process artifacts on the BeyondTrust appliance host: `/etc/passwd`, `lastlog`, `auth.log` or `/var/log/secure`, and running process list (`ps aux`) captured as a memory-safe snapshot before patch application — a sophisticated attacker who achieved RCE via the pre-auth bypass may have implanted a backdoor process or created a local OS account on the appliance host itself, separate from the BeyondTrust application layer.

Per-Action IR Details

Step 1: Containment — Identify all instances of BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA) appliances in your environment. If internet-facing instances cannot be patched immediately, restrict external access at the network perimeter or via WAF/IPS rules until the patch is applied. Consult BeyondTrust advisory BT26-02 (https://www.beyondtrust.com/trust-center/security-advisories/bt26-02) for interim workaround guidance.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: For teams without centralized asset management, run `nmap -p 443,8200,8443 --open -sV` to fingerprint BeyondTrust appliance management ports. Block inbound traffic to those ports at the perimeter firewall using an explicit deny ACL until BT26-02 patches are applied. Document every identified instance with IP, hostname, and whether it is internet-facing before proceeding.

Evidence: Before restricting network access, capture full netflow or firewall session table exports showing active connections to BeyondTrust appliance management ports (typically TCP 443, 8200, 8443) to preserve evidence of any pre-containment unauthorized sessions. Run `netstat -ano` or `ss -tulnp` on the appliance host (if accessible) and export results. Capture the appliance's current active session list from the BeyondTrust admin console before ACL changes terminate live sessions — these session records may be the only record of an attacker's foothold established

via the pre-auth bypass.

Step 2: Detection — Review appliance access logs for unauthenticated or anomalous session activity prior to patch application, focusing on MITRE T1133 (External Remote Services) and T1190 (Exploit Public-Facing Application) patterns. Look for access attempts that bypassed normal authentication flows, unexpected session initiations from unknown IPs, and any privilege escalation events on systems managed through these appliances. Correlate with firewall and proxy logs for external access to appliance management ports. Enable audit logging per NIST AU-2 and AU-12 if not already active.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, export BeyondTrust RS/PRA appliance access logs (typically located under `/var/log/beyondtrust/` on Linux-based appliances or via the admin console export function) and parse with `grep` or PowerShell `Select-String` for HTTP 200 responses on authentication endpoints (`/login`, `/api/auth`) that lack a corresponding valid credential submission in the preceding request sequence — a hallmark of pre-auth bypass exploitation. Cross-reference source IPs against threat intel feeds using the free Shodan CLI (`shodan host `) to identify known malicious infrastructure. Use Zeek or Wireshark pcap analysis on the appliance's management interface traffic to identify sessions that progressed to authenticated state without a valid TLS client certificate or credential exchange.

Evidence: Capture the following before any log rotation or appliance restart: BeyondTrust appliance web access logs showing HTTP method, URI path, source IP, HTTP response code, and session token for all requests to authentication and API endpoints in the 90 days preceding discovery; firewall flow logs for inbound connections to appliance management ports from external IPs; any BeyondTrust audit trail exports showing session creation events with missing or null authentication context fields; and memory image of the appliance OS if live compromise is suspected, to recover attacker-injected session tokens or process artifacts from the pre-auth bypass exploitation.

Step 3: Eradication — Apply the patches specified in BeyondTrust advisory BT26-02. Specific patch identifiers and version upgrade paths should be sourced directly from the advisory, as version-level details were not available in the source data provided. After patching, rotate credentials for all accounts that had access to the affected appliances, consistent with D3-CRO (Credential Rotation), given the possibility that pre-auth bypass may have permitted unauthorized session establishment.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST AC-2 (Account Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For teams performing manual patch application: download the BT26-02 patch from the BeyondTrust customer portal, verify the SHA-256 hash of the installer against the advisory-published value before applying, and document the pre- and post-patch appliance version strings from the admin console. For credential rotation without a PAM tool, use a scripted password reset workflow: export all accounts from the BeyondTrust admin console, generate unique passwords meeting complexity requirements via `openssl rand -base64 24`, and force reset via the appliance API or admin console for every account, prioritizing service accounts and any accounts with administrative roles on managed endpoints.

Evidence: Before applying the BT26-02 patch or rotating credentials — both of which alter live appliance state — capture: a full export of the BeyondTrust session audit log (all sessions, all users, full date range available) to preserve any attacker-established session records that patch application may overwrite; a snapshot of all current active sessions in the appliance console; a list of all accounts currently provisioned in the appliance with their role and last-login timestamp; and for Linux-based appliances, `/etc/passwd`, `/etc/shadow` (hashed), and `last`/`lastlog` outputs to detect any OS-level accounts created by an attacker who escalated from the BeyondTrust pre-auth bypass.

Step 4: Recovery — After patching, verify appliance version numbers against BT26-02 remediated version requirements. Confirm authentication controls are functioning correctly by testing unauthenticated access attempts in a controlled manner. Monitor appliance logs for any continued anomalous activity for at least 30 days post-remediation per AU-6 (Audit Record Review, Analysis, and Reporting). Validate that no unauthorized accounts or sessions persist on managed endpoints.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AC-2 (Account Management), NIST AC-3 (Access Enforcement), CIS 5.1 (Establish and Maintain an Inventory of Accounts)

Compensating: Without enterprise EDR on managed endpoints, use osquery (`SELECT * FROM logged_in_users; SELECT * FROM last;`) across all endpoints that were managed through the BeyondTrust appliances during the exposure window to detect persistence artifacts left by an attacker who leveraged the pre-auth bypass to reach managed systems. Verify appliance patch status by querying the admin console version string and comparing against BT26-02's remediated version table. For controlled authentication testing, use `curl -k -X POST https:///api/auth --data '{}'` to confirm the endpoint now returns a proper 401/403 rather than the bypass-susceptible response observed pre-patch.

Evidence: Before re-enabling full external access to the patched appliances, capture: post-patch appliance version string and configuration export as a baseline for future integrity comparison; a fresh account inventory export from both the BeyondTrust admin console and from all managed endpoint systems (Windows: `net localgroup administrators`; Linux: `getent group sudo`) to identify any accounts created during the exploitation window; and Windows Security Event Log Event ID 4720 (account created) and Event ID 4728 (member added to security-enabled global group) from managed endpoints for the period spanning the vulnerability exposure window.

Step 5: Post-Incident — Conduct a review of privileged remote access architecture. Assess whether BeyondTrust appliances are segmented from direct internet exposure and require MFA for all administrative access per CIS 6.5 and D3-MFA. Review account inventory per CIS 5.1 and enforce least privilege per NIST AC-6. Document lessons learned and update the vulnerability management process per CIS 7.1 to include faster patching SLAs for pre-authentication critical vulnerabilities in privileged access tooling.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST AC-6 (Least Privilege), NIST AC-17 (Remote Access), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: For teams without a dedicated PAM platform to enforce architectural segmentation: document a network diagram showing BeyondTrust appliance placement relative to DMZ and internal segments, then create firewall ACL rules restricting appliance management interface access to a dedicated jump host IP only. Implement MFA for BeyondTrust admin access using the appliance's built-in TOTP/SAML integration (no additional cost) and validate the configuration is enforced by attempting admin login without MFA from the jump host. Update the internal vulnerability management tracking spreadsheet (or ticketing system) to add a dedicated SLA field for 'pre-authentication critical — PAM/remote access tooling' with a 24-hour patch-or-isolate SLA.

Evidence: For the lessons-learned record, preserve: the full timeline of BeyondTrust appliance exposure (first internet-facing date through patch application date) correlated against threat intel for known BT26-02 exploitation activity; the complete account audit from Recovery (Step 4) as evidence of scope; firewall and appliance log exports covering the full exposure window for potential regulatory disclosure support; and the pre-patch architecture diagram showing appliance network placement to document the control gap that allowed internet exposure of a pre-auth-vulnerable privileged access management appliance.

Detection Guidance

Review BeyondTrust RS and PRA appliance access and authentication logs for the period before patch application. Indicators of attempted exploitation include: unauthenticated requests that successfully initiated sessions or received 200-series responses on appliance management interfaces; access from external IPs not associated with known administrators; session activity at unusual hours or from geolocations inconsistent with your workforce. If your SIEM ingests appliance syslog, query for authentication events with null or empty credential fields that resulted in successful session establishment. Also review downstream systems managed through these appliances for unauthorized configuration changes or new account creation, consistent with post-exploitation activity under MITRE T1133. No specific IOC patterns (hashes, IPs, domains) were available in the source data; monitor BeyondTrust's advisory BT26-02 and threat intelligence feeds for attacker infrastructure if active exploitation is reported. Align log collection with NIST AU-3 (Content of Audit Records) to ensure records capture source IP, user identity, timestamp, and outcome for each session.

Framework Mappings

MITRE-ATTACK

- **T1133** — External Remote Services
- **T1190** — Exploit Public-Facing Application

NIST-800-53R5

- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SC-7** — Boundary Protection
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **IA-8** — Identification and Authentication (Non-Organizational Users)

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

- **CC9.2** — Manages risks associated with vendors and business partners
- **CC6.3** — Authorizes, modifies, or removes access

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.21** — Managing information security in the ICT supply chain
- **A.5.23** — Information security for use of cloud services

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1133	External Remote Services	Persistence
T1190	Exploit Public-Facing Application	Initial-Access

Sources

Source	URL	Tier
The Hacker News	https://thehackernews.com/2026/07/beyondtrust-patches-critical-auth...	T2
(consolidated)	https://www.bleepingcomputer.com/news/security/beyondtrust-warns-of...	T2
BT26-02 - BeyondTrust	https://www.beyondtrust.com/trust-center/security-advisories/bt26-02	T3
BeyondTrust Patches Critical Remote Support and Privileged ...	https://cyberpress.org/beyondtrust-remote-support-privileged-access/	T3
Critical BeyondTrust Flaws Allow Attackers Bypass Access ...	https://cybersecuritynews.com/beyondtrust-vulnerabilities/	T3

Generated 2026-07-07 16:14 UTC by TJS Security Command Center