INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-21 18:37 UTC

CVE-2026-1731: Active RCE Exploitation in Bomgar RMM Turns Privileged Access Into Ransomware Launchpad

CVE VULNERABILITY | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CVE-2026-0061
Type	CVE Vulnerability
CVE ID	CVE-2026-1731
Severity	CRITICAL
CVSS Base Score	9.5
EPSS Score	0.8150 (99th percentile)
Affected Products	BeyondTrust (Bomgar) Remote Monitoring and Management (RMM), specific version range unverified from available source data
Published	2026-04-21T11:29:17
Discovery Source	Rss

Executive Summary

A critical unauthenticated remote code execution vulnerability in BeyondTrust's Bomgar Remote Monitoring and Management platform is under active exploitation. Attackers are using compromised RMM infrastructure as a launchpad to deploy ransomware and move laterally across all managed endpoints. A single compromised RMM instance grants attackers access equivalent to the RMM's privileges across every device it manages, enabling simultaneous ransomware deployment. Organizations running Bomgar RMM face immediate, high-probability risk of enterprise-wide ransomware deployment and operational shutdown.

Technical Analysis

CVE-2026-1731 is a critical unauthenticated RCE vulnerability in BeyondTrust's Bomgar Remote Monitoring and Management platform (CVSS base: 9.5; EPSS: 0.815, 99th percentile). The vulnerability allows pre-authentication code execution through privileged RMM communication channels. Underlying weaknesses map to CWE-78 (OS command injection), CWE-94 (code injection), and CWE-20 (improper input validation). Active exploitation has been observed in the wild; specific threat actor attribution is not yet available. MITRE ATT&CK technique coverage includes T1072 (Software Deployment Tools), T1210 (Exploitation of Remote

Services), T1059 (Command and Scripting Interpreter), T1570 (Lateral Tool Transfer), T1486 (Data Encrypted for Impact), T1195 (Supply Chain Compromise), and T1021 (Remote Services). The RMM trust model amplifies blast radius: successful exploitation grants attacker access equivalent to the RMM agent's elevated privileges across all managed endpoints. Affected version range pending BeyondTrust official confirmation; consult vendor advisory and NVD directly for scope details. CISA KEV listing status unconfirmed at time of publication.

Action Checklist

1. Step 1: Containment. Immediately isolate internet-facing Bomgar RMM infrastructure. Restrict RMM management console access to specific trusted IP ranges via firewall ACLs. Suspend non-essential RMM agent connections until patch status is confirmed. Check BeyondTrust's security advisory portal directly for emergency guidance on affected versions and remediation options.
2. Step 2: Detection. Review RMM server logs for unauthenticated connection attempts, unexpected process spawning from the RMM service account, and outbound connections to unknown IPs from managed endpoints. Look for T1059 indicators: unexpected cmd.exe, powershell.exe, or script interpreter execution chains parented to the Bomgar RMM process. Query EDR telemetry for lateral movement from RMM agent processes (T1021, T1570). Check for ransomware staging artifacts (T1486): volume shadow copy deletion, bulk file encryption events, abnormal disk I/O.
3. Step 3: Eradication. Apply BeyondTrust's official patch immediately upon release (check BeyondTrust security advisory portal for availability and affected version confirmation). If patch is unavailable or your version status remains unclear, disable the RMM service on exposed hosts and revert to manual management until vendor confirmation is received. Remove any malicious artifacts identified during detection, including persistence mechanisms and dropped payloads.
4. Step 4: Recovery. After patching, verify RMM agent integrity on all managed endpoints. Re-baseline expected process trees and network behavior for RMM services. Monitor for re-exploitation attempts for a minimum of 72 hours post-patch. Confirm no ransomware staging artifacts remain before restoring full RMM connectivity. Validate backup integrity before resuming normal operations.
5. Step 5: Post-Incident. Conduct a trust-model review of all RMM platforms in the environment: assess whether RMM agents hold more privilege than operationally required and reduce to least-privilege where possible. Implement network segmentation to limit lateral movement potential from RMM infrastructure. Review supply chain and third-party access pathways (T1195 exposure). Add RMM process behavior monitoring as a permanent detection rule in your SIEM and EDR.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to executive leadership, legal counsel, and external IR retainer immediately if any managed endpoint shows confirmed ransomware execution (encrypted files, ransom note dropped, VSS deletion confirmed), if PII or PHI data stores are accessible to managed endpoints (triggering HIPAA breach notification assessment under 45 CFR §164.410 or state breach notification statutes), or if the organization lacks internal capability to isolate all Bomgar RMM agent connections within 2 hours of detection.

Recovery Notes	Before restoring Bomgar RMM connectivity to any managed endpoint, confirm three conditions: the RMM server is running the BeyondTrust-patched version (verify against the official BeyondTrust security advisory hash), the managed endpoint shows no ransomware staging artifacts in the 72-hour post-patch Sysmon monitoring window, and all backup snapshots used for recovery have been integrity-validated via SHA-256 hash comparison against pre-incident checksums. Maintain elevated Sysmon and network monitoring on the Bomgar RMM server for a minimum of 14 days post-recovery, as threat actors exploiting RMM infrastructure commonly install secondary persistence (scheduled tasks, additional remote access tools) during the initial compromise window that may survive a service-level patch if the host was not fully re-imaged. If any managed endpoint was confirmed to execute ransomware payloads, treat that endpoint as fully compromised and reimage from a validated clean backup rather than attempting in-place remediation.
Forensic Artifacts	Bomgar RMM server application logs at C:\ProgramData\BeyondTrust\RMM\logs\ — review for unauthenticated HTTP requests to the RMM API surface, anomalous POST body sizes indicative of exploit payload delivery, and session tokens issued without prior valid authentication handshake; these logs are the primary evidence of the CVE-2026-1731 unauthenticated RCE trigger. | Windows Security Event Log Event ID 4688 (Process Creation) with command-line auditing enabled on the Bomgar RMM server — filter on ParentProcessName matching the Bomgar service executable to identify attacker-controlled command interpreter chains (cmd.exe, powershell.exe) spawned directly from the RMM service process as the first post-exploitation action. | Sysmon Event ID 3 (Network Connection) logs from all managed endpoints — filter on source process matching Bomgar agent executables making outbound connections to non-BeyondTrust IP ranges during the exploitation window, which evidences the RMM agent trust relationship being abused for C2 callback and lateral movement (MITRE T1021, T1570). | Volume Shadow Copy metadata via 'vssadmin list shadows' output and Sysmon Event ID 1 logs for vssadmin.exe, wbadmin.exe, and bcdedit.exe execution — presence of shadow copy deletion commands executed under the Bomgar service account SID directly evidences ransomware staging (MITRE T1486) initiated through the compromised RMM infrastructure. | Memory dump of the Bomgar RMM service process (BeyondTrustRMM.exe or equivalent) captured via ProcDump at time of containment — in-memory forensics will reveal injected shellcode, decoded payload stages, or Cobalt Strike/Meterpreter artifacts resident in the process heap that would not appear in on-disk artifact scans, preserving evidence of the exploit mechanism before process termination.

Per-Action IR Details

Step 1: Containment — Immediately isolate internet-facing Bomgar RMM infrastructure. Restrict RMM management console access to specific trusted IP ranges via firewall ACLs. Suspend non-essential RMM agent connections until patch status is confirmed. Check BeyondTrust's security advisory portal directly for emergency guidance on affected versions.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), NIST AC-17 (Remote Access), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices), CIS 12.2 (Establish and Maintain a Secure Network Architecture)

Compensating: On Windows hosts running the Bomgar RMM agent or server component, immediately block inbound/outbound traffic on the Bomgar listening port (default TCP 443/8200) using Windows Firewall: `netsh advfirewall firewall add rule name='BLOCK_BOMGAR' dir=in action=block protocol=tcp localport=443,8200`. On Linux/network perimeter: `iptables -I INPUT -p tcp --dport 8200 -j DROP`. For a 2-person team with no NGFW, use a

host-based block on the RMM server itself and physically segment the management VLAN by disabling the switch uplink port until ACLs are confirmed. Document all blocked connections with timestamps per NIST 800-61r3 §3.3 evidence preservation requirements.

Evidence: Before isolating, capture a full netstat snapshot of the Bomgar RMM server to document all active sessions: `netstat -anob > C:\IR\bomgar_netstat_precontainment.txt`. Dump the Bomgar RMM service process memory using ProcDump (`procdump -ma C:\IR\bomgar_pre_isolation.dmp`) to preserve in-memory exploit artifacts before the process is killed or the host is isolated. Export Windows Security Event Log and the Bomgar server application logs (default path: `C:\ProgramData\BeyondTrust\RMM\logs\`) before network isolation severs access. Capture current active RMM sessions from the admin console export if accessible — this identifies which managed endpoints were connected at time of compromise.

Step 2: Detection — Review RMM server logs for unauthenticated connection attempts, unexpected process spawning from the RMM service account, and outbound connections to unknown IPs from managed endpoints. Look for T1059 indicators: unexpected cmd.exe, powershell.exe, or script interpreter execution chains parented to the Bomgar RMM process. Query EDR telemetry for lateral movement from RMM agent processes (T1021, T1570). Check for ransomware staging artifacts (T1486): volume shadow copy deletion, bulk file encryption events, abnormal disk I/O.

NIST Phase: Detection Analysis

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

Controls: NIST IR-4 (Incident Handling), NIST IR-5 (Incident Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon with a configuration tuned for parent-process anomalies on the Bomgar RMM server and all managed endpoints (use the SwiftOnSecurity or olafhartong Sysmon config as a baseline). Query Sysmon Event ID 1 (Process Create) filtering for `ParentImage` containing the Bomgar service executable (typically `BeyondTrustRMM.exe` or `RepairTech.exe`) spawning `cmd.exe`, `powershell.exe`, `wscript.exe`, or `mshta.exe`: `Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational' | Where-Object {$_.Id -eq 1 -and $_.Message -match 'BeyondTrust' -and $_.Message -match 'cmd.exe|powershell'}`. For volume shadow copy deletion (ransomware staging), query Sysmon Event ID 1 for `vssadmin.exe delete shadows` or `wmic shadowcopy delete`. Use osquery to hunt lateral movement: `SELECT * FROM process_open_sockets WHERE pid IN (SELECT pid FROM processes WHERE name LIKE '%BeyondTrust%')`. Apply the public Sigma rule for T1059 command interpreter abuse adapted to Bomgar's process name.

Evidence: Collect Bomgar RMM server access logs from `C:\ProgramData\BeyondTrust\RMM\logs\` — look for HTTP 200 responses to unauthenticated API endpoints or abnormal POST request sizes indicative of exploit payload delivery. Pull Windows Security Event Log Event ID 4688 (Process Creation) with full command-line logging enabled, filtering on processes parented to the Bomgar service account SID. Collect Sysmon Event ID 3 (Network Connection) for outbound connections initiated by the Bomgar service process to non-BeyondTrust IP ranges — these represent C2 beaconing or ransomware staging callbacks. On managed endpoints, capture Windows Security Event ID 7045 (New Service Installed) and 4697 (Service Installed) within the exploitation window to identify persistence mechanisms deployed via RMM. Export VSS snapshot metadata (`vssadmin list shadows`) before any remediation to document the pre-ransomware state.

Step 3: Eradication — Apply BeyondTrust's official patch immediately upon release; confirm the specific patched version directly with BeyondTrust's security advisory (no patch version was independently verified from available source data). If patch is unavailable, disable the RMM service on exposed hosts and revert to manual management until remediation is confirmed. Remove any malicious artifacts identified during detection, including persistence mechanisms and dropped payloads.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST IR-4 (Incident Handling), NIST CM-7 (Least Functionality), NIST SI-3 (Malicious Code Protection), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4

(Perform Automated Application Patch Management)

Compensating: Until BeyondTrust releases the official patch, disable the Bomgar RMM service on all internet-exposed servers: `sc stop 'BeyondTrust RMM' && sc config 'BeyondTrust RMM' start=disabled`. For artifact removal without EDR: use Autoruns (Sysinternals) to identify persistence entries written by the Bomgar service account — filter on the service account username and review Run keys, scheduled tasks, and service entries added within the exploitation window. Hunt dropped payloads using ClamAV with an updated signature database scanning `C:\ProgramData\BeyondTrust\`, `C:\Windows\Temp\`, and `%APPDATA%` of the service account. Write a YARA rule targeting common ransomware staging binaries (e.g., Cobalt Strike beacon signatures, known ransomware dropper strings) and scan all managed endpoints before re-enabling connectivity. Document every artifact removed with hash, path, and timestamp per NIST 800-61r3 §3.4 eradication evidence requirements.

Evidence: Before removing any artifacts, create forensic disk images of the Bomgar RMM server using FTK Imager or `dd` to preserve the exploitation evidence chain. Collect all files created or modified in the Bomgar installation directory and `%TEMP%` paths under the service account within the exploitation window: `forfiles /P C:\ProgramData\BeyondTrust /S /D + /C "cmd /c echo @path @fdate @ftime"`. Export the Windows Registry hive `HKLM\SYSTEM\CurrentControlSet\Services` to document any new services registered by the attacker. Capture scheduled task XML exports (`schtasks /query /fo LIST /v > C:\IR\scheduled_tasks.txt`) to document persistence mechanisms. Hash all collected artifacts (SHA-256) before deletion to support downstream threat intelligence sharing and potential law enforcement requirements.

Step 4: Recovery — After patching, verify RMM agent integrity on all managed endpoints. Re-baseline expected process trees and network behavior for RMM services. Monitor for re-exploitation attempts for a minimum of 72 hours post-patch. Confirm no ransomware staging artifacts remain before restoring full RMM connectivity. Validate backup integrity before resuming normal operations.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CP-9 (System Backup), NIST CP-10 (System Recovery and Reconstitution), NIST SI-2 (Flaw Remediation), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 11.4 (Establish and Maintain an Isolated Instance of Recovery Data)

Compensating: Verify Bomgar RMM agent binary integrity on managed endpoints by comparing SHA-256 hashes of deployed agent executables against the BeyondTrust-published hash from the official release notes. Use PowerShell across all managed hosts: `Get-FileHash 'C:\Program Files\BeyondTrust\Remote Support\*' -Algorithm SHA256 | Export-Csv C:\IR\agent_integrity.csv`. Re-establish the legitimate process tree baseline for Bomgar services using Sysmon Event ID 1 data collected from a known-clean reference host patched to the new version. For backup integrity validation without enterprise backup tooling, use `certutil -hashfile SHA256` to verify backup file hashes against pre-incident checksums. Monitor Sysmon Event ID 1 and 3 on the Bomgar RMM server continuously for the 72-hour window, alerting on any child process spawned from the Bomgar service process.

Evidence: Before restoring RMM connectivity, run a final sweep of all previously managed endpoints for ransomware staging indicators: query Sysmon Event ID 1 for `vssadmin`, `wbadmin`, or `bcdedit` execution (backup deletion precursors) and Event ID 11 (File Create) for mass creation of files with encrypted-file extensions (`.locked`, `.encrypted`, `.ryk`, `.conti`, etc.) in user directories. Validate that no Bomgar agent on managed endpoints is communicating with non-BeyondTrust infrastructure by reviewing Sysmon Event ID 3 logs for the 72-hour post-patch monitoring window. Document the recovery state with a signed attestation log capturing: patch version applied, agent hash verification results, backup validation checksums, and monitoring period outcomes — this serves as the audit trail required by NIST AU-10 (Non-Repudiation).

Step 5: Post-Incident — Conduct a trust-model review of all RMM platforms in the environment: assess whether RMM agents hold more privilege than operationally required and reduce to least-privilege where possible. Implement network segmentation to limit lateral movement potential from RMM infrastructure. Review supply chain and third-party access pathways (T1195 exposure). Add RMM process behavior monitoring as a permanent detection rule in your SIEM and EDR.

NIST Phase: Post Incident

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

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST AC-6 (Least Privilege), NIST SC-7 (Boundary Protection), NIST RA-3 (Risk Assessment), NIST SA-9 (External System Services), NIST SI-4 (System Monitoring), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: Conduct the RMM privilege audit using a PowerShell script querying local Administrator group membership on all managed endpoints: `Invoke-Command -ComputerName (Get-Content endpoints.txt) -ScriptBlock {net localgroup administrators}` — identify where the Bomgar service account holds local admin rights that can be reduced. Convert the Bomgar process behavior detection into a permanent Sigma rule targeting `ParentImage|endswith: 'BeyondTrustRMM.exe'` with child processes of `cmd.exe`, `powershell.exe`, or `mshta.exe` and publish to your log aggregator (even a syslog server running Graylog CE qualifies). For network segmentation without enterprise SDN, use VLAN tagging on the management switch to isolate the RMM infrastructure subnet and enforce ACLs at the router/L3 switch level restricting RMM server outbound to only BeyondTrust update CDN ranges and inbound to only the dedicated admin jump host IP.

Evidence: Produce a post-incident lessons-learned report documenting: the initial attack vector (unauthenticated RCE entry point on the Bomgar RMM console), the lateral movement path from RMM server to managed endpoints via the agent trust relationship (MITRE ATT&CK T1021, T1570), the ransomware staging sequence observed (T1486 artifacts), and the detection gap that allowed dwell time before identification. Preserve the full forensic artifact set (memory dumps, disk images, log exports, network captures) for a minimum of 12 months per NIST AU-11 (Audit Record Retention) to support potential regulatory notification timelines and threat intelligence sharing. Document all third-party RMM vendors with access to the environment per NIST SA-9 (External System Services) and submit IOCs (C2 IPs, malicious hashes, exploit URI patterns from Bomgar access logs) to the MS-ISAC or appropriate sector ISAC.

Detection Guidance

Focus detection on the Bomgar RMM service process as a parent. Flag any child process creation from the RMM service that includes cmd.exe, powershell.exe, wscript.exe, mshta.exe, or other script interpreters (T1059). In Windows Event Logs, look for Event ID 4688 (process creation) with parent process matching the Bomgar/BeyondTrust RMM executable. Search SIEM for outbound connections from RMM infrastructure to new or uncategorized external IPs, particularly over high ports or to geographies inconsistent with vendor infrastructure. For ransomware staging, watch for Event ID 7036 (Volume Shadow Copy service state change), vssadmin.exe delete shadows commands, and WMI-based shadow copy deletion. For lateral movement (T1021, T1570), alert on file copy or execution events originating from the RMM agent account to remote systems. EPSS score of 0.815 (99th percentile) indicates very high exploitation probability - prioritize this over lower-probability alerts. No confirmed IOCs were available in the source data at time of publication; consult BeyondTrust's advisory and threat intelligence feeds for emerging indicators.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`none confirmed`	No IOCs were available in the source data at time of publication. Monitor BeyondTrust's official security advisory, NVD entry for CVE-2026-1731, and threat intelligence feeds for emerging indicators.	LOW

Framework Mappings

MITRE-ATTACK

- **T1570** — Lateral Tool Transfer
- **T1486** — Data Encrypted for Impact
- **T1059** — Command and Scripting Interpreter
- **T1210** — Exploitation of Remote Services
- **T1195** — Supply Chain Compromise
- **T1072** — Software Deployment Tools
- **T1021** — Remote Services

NIST-800-53R5

- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-6** — Least Privilege
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SA-9** — External System Services
- **SR-2** — Supply Chain Risk Management Plan
- **SR-3** — Supply Chain Controls and Processes
- **AC-17** — Remote Access
- **AC-3** — Access Enforcement
- **IA-2** — Identification and Authentication (Organizational Users)
- **SI-10** — Information Input Validation
- **IR-4** — Incident Handling
- **AT-2** — Literacy Training and Awareness
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

- **A03:2021** — Injection

CIS-V8

- **2.5** — Allowlist Authorized Software
- **16.10** — Apply Secure Design Principles in Application Architectures
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **8.2** — Collect Audit Logs

ISO-27001-2022

- **A.8.26** — Application security requirements
- **A.5.29** — Information security during disruption
- **A.8.8** — Management of technical vulnerabilities
- **A.5.21** — Managing information security in the ICT supply chain

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **DE.CM-01** — Networks and network services are monitored
- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan

SOC2-TSC

- **CC9.2** — Manages risks associated with vendors and business partners

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1570	Lateral Tool Transfer	Lateral-Movement
T1486	Data Encrypted for Impact	Impact
T1059	Command and Scripting Interpreter	Execution
T1210	Exploitation of Remote Services	Lateral-Movement
T1195	Supply Chain Compromise	Initial-Access
T1072	Software Deployment Tools	Execution
T1021	Remote Services	Lateral-Movement

Sources

Source	URL	Tier
Security News	https://www.darkreading.com/cyberattacks-data-breaches/surge-bomgar...	T3
CVE-2026-1731 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-1731	T1
CVE-2026-1731: Critical Unauthenticated Remote Code ... - Rapid7	https://www.rapid7.com/blog/post/etr-cve-2026-1731-critical-unauthe...	T3
CVE-2026-1731 | Arctic Wolf	https://arcticwolf.com/resources/blog/cve-2026-1731/	T3
BeyondTrust RCE vulnerability: CVE-2026-1731 - runZero	https://www.runzero.com/blog/beyondtrust-appliances/	T3

Generated 2026-04-21 18:37 UTC by TJS Security Command Center