INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-10 07:26 UTC

Veeam Backup & Replication RCE Vulnerability CVE-2026-44963 Allows Authenticated Domain Users to Execute Remote Code

CVE VULNERABILITY | HIGH | CVSS 8.8

SCC Item ID	SCC-CVE-2026-0285
Type	CVE Vulnerability
CVE ID	CVE-2026-44963
Severity	HIGH
CVSS Base Score	8.8
Affected Products	Veeam Backup & Replication (versions prior to 12.3.2 build fixes; patched in 12.3.2)
Published	17 hours ago
Discovery Source	Serper

Executive Summary

A high-severity remote code execution vulnerability (CVE-2026-44963, CVSS 8.8) in Veeam Backup & Replication allows any authenticated domain user to execute arbitrary code on backup servers. Organizations running versions prior to 12.3.2 are exposed, and the bar for exploitation is low - domain user credentials are sufficient. Backup infrastructure is a primary ransomware target; compromise of backup servers can eliminate recovery options and extend breach impact across the enterprise.

Technical Analysis

CVE-2026-44963 is a remote code execution vulnerability in Veeam Backup & Replication affecting all versions prior to the 12.3.2 build fix (KB4743). The vulnerability is rooted in CWE-94 (improper code neutralization enabling code injection) and CWE-269 (improper privilege management), allowing an authenticated domain user, with no elevated permissions required, to execute arbitrary remote code against the backup server. MITRE ATT&CK mapping: T1210 (Exploitation of Remote Services), T1078.002 (Valid Accounts: Domain Accounts), T1570 (Lateral Tool Transfer). No public exploit code or active exploitation is confirmed in available source data; CISA KEV listing is not confirmed. EPSS data was not available in the source record. Patch: upgrade to Veeam Backup & Replication 12.3.2 per vendor release notes. Note: Verify the official Veeam KB article before implementation; human validation is recommended before treating patch guidance as confirmed.

Action Checklist

1. Step 1: Containment. Immediately restrict network access to Veeam Backup & Replication servers (TCP 9392, 9401, and other Veeam service ports) to dedicated backup admin workstations only. Remove domain user permissions to backup server interfaces where not operationally required. Reference: NIST AC-3 (Access Enforcement), NIST AC-6 (Least Privilege), CIS 4.4 (Implement and Manage a Firewall on Servers).
2. Step 2: Detection. Query authentication and application logs on Veeam backup servers for successful logons by non-backup-admin domain accounts (Windows Security Event ID 4624, logon type 3 or 10). Look for anomalous process spawning from Veeam service accounts (Veeam.Backup.Service.exe, Veeam.Backup.Manager.exe) in Windows Event ID 4688 or EDR telemetry. Flag any lateral tool transfers or staged payloads in Veeam backup repositories. Reference: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs).
3. Step 3: Eradication. Apply the Veeam Backup & Replication 12.3.2 patch per vendor release notes on all affected backup servers. Validate the installed build number matches the 12.3.2 fixed build post-upgrade. Audit and revoke any domain user accounts granted access to backup server management interfaces beyond operationally required roles. Reference: NIST SI-2 (Flaw Remediation), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management).
4. Step 4: Recovery. After patching, verify backup job integrity by running a test restore from recent backup chains. Confirm no unauthorized scheduled tasks, services, or startup entries were added to backup servers (Windows Event ID 4698 for scheduled tasks, 7045 for service creation). Review system files and executables on backup servers for unauthorized modifications using file integrity monitoring tools. Monitor Veeam service account activity for 30 days post-remediation. Reference: NIST AU-6, CIS 8.2.
5. Step 5: Post-Incident. Review whether domain user accounts should have any access to backup management infrastructure; implement dedicated, non-domain backup admin accounts where architecture permits. Enforce MFA on all backup server administrative access (CIS 6.5: Require MFA for Administrative Access; NIST IA-2: Authentication). Rotate credentials for any service accounts with access to backup infrastructure (NIST IA-4: Identifier Management). Document this gap against NIST AC-6 (Least Privilege) and AC-5 (Separation of Duties) and include in the next risk assessment cycle.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to senior IR leadership and legal/compliance immediately if Windows Event ID 4688 or Sysmon Event ID 1 confirms a child process spawned from Veeam.Backup.Service.exe or Veeam.Backup.Manager.exe, if backup repository data shows signs of encryption or deletion consistent with ransomware pre-positioning, or if the organization holds PII, PHI, or PCI-scoped data in systems backed up by the compromised Veeam server (triggering breach notification assessment under applicable regulations).

Recovery Notes	Before restoring any systems from Veeam backup chains, validate backup integrity via SureBackup or manual restore test to confirm backup data was not encrypted or poisoned by an attacker who leveraged CVE-2026-44963 to access backup repositories prior to detection — compromised backups used for recovery can re-introduce attacker persistence. Monitor Veeam service account authentication events (Windows Security Event ID 4624, logon types 3, 4, and 5) and process creation from Veeam parent processes (Sysmon Event ID 1) for a minimum of 30 days post-patch, as threat actors who achieved RCE may have implanted scheduled tasks or services designed to survive the patch cycle. Verify that all backup jobs complete successfully post-patch and that no unauthorized backup jobs, repositories, or scale-out backup repository (SOBR) targets were added during the exposure window.
Forensic Artifacts	Windows Security Event Log (Event ID 4624, Logon Type 3/10) on the Veeam server — identifies non-admin domain user authentication events that represent the low-bar exploitation entry point specific to CVE-2026-44963's authenticated-domain-user attack vector. | Sysmon Event ID 1 (Process Creation) or Windows Event ID 4688 filtered on ParentImage = Veeam.Backup.Service.exe or Veeam.Backup.Manager.exe — child process spawning from these Veeam service processes is the primary forensic indicator of successful RCE exploitation of CVE-2026-44963. | Veeam application logs at C:\ProgramData\Veeam\Backup\Logs\ — these logs record API calls, job creation, and repository access events; unauthorized job creation or repository enumeration would appear here if an attacker used the RCE to interact with Veeam's backup management functions. | Windows Event IDs 7045 (New Service Installed) and 4698 (Scheduled Task Created) from the Security and System logs covering the full vulnerability exposure window — these are the most operationally significant persistence artifacts an attacker would leave after achieving RCE on a backup server targeted as ransomware pre-positioning infrastructure. | Veeam backup repository catalog and job history — specifically, examine for unauthorized backup job deletions, repository target additions, or encryption of .VBK/.VIB/.VRB backup files within the repository storage path, which would indicate the attacker leveraged CVE-2026-44963 access to sabotage recovery options as a ransomware precursor action.

Per-Action IR Details

Step 1: Containment — Immediately restrict network access to Veeam Backup & Replication servers (TCP 9392, 9401, and other Veeam service ports) to dedicated backup admin workstations only. Remove domain user permissions to backup server interfaces where not operationally required. Reference: NIST AC-3 (Access Enforcement), NIST AC-6 (Least Privilege), CIS 4.4 (Implement and Manage a Firewall on Servers).

NIST Phase: Containment

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

Controls: NIST AC-3 (Access Enforcement), NIST AC-6 (Least Privilege), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: On the Veeam backup server, run: netsh advfirewall firewall add rule name='Veeam RCE Block CVE-2026-44963' protocol=TCP dir=in localport=9392,9401 action=block. Then create an allow rule scoped to backup admin workstation IPs only. Enumerate current connections first: netstat -ano | findstr '9392\|9401' to capture active sessions before blocking. No SIEM required — this is host-firewall enforcement executable by one analyst in under 10 minutes.

Evidence: Before restricting ports, capture a full netstat snapshot (netstat -ano > veeam_active_connections_.txt) and export Windows Firewall logs (%SystemRoot%\System32\LogFiles\Firewall\pfirewall.log) to document which source IPs were connected to TCP 9392 and 9401 at time of containment. These connection records establish the scope of potential exploiters — CVE-2026-44963 requires an authenticated inbound connection to Veeam service ports to trigger RCE.

Step 2: Detection — Query authentication and application logs on Veeam backup servers for successful logons by non-backup-admin domain accounts (Windows Security Event ID 4624, logon type 3 or 10). Look for anomalous process spawning from Veeam service accounts (Veeam.Backup.Service.exe, Veeam.Backup.Manager.exe) in Windows Event ID 4688 or EDR telemetry. Flag any lateral tool transfers or staged payloads in Veeam backup repositories. Reference: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs).

NIST Phase: Detection Analysis

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

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

Compensating: Deploy Sysmon with a configuration that captures process creation (Event ID 1) and network connections (Event ID 3) — filter on ParentImage containing 'Veeam.Backup.Service.exe' or 'Veeam.Backup.Manager.exe' with child processes that are not expected Veeam binaries (e.g., cmd.exe, powershell.exe, wscript.exe). Use the following PowerShell one-liner to query Security logs: Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4624 -and $_.Message -match 'LogonType.*3|LogonType.*10'} | Select-Object TimeCreated, Message | Export-Csv veeam_logons.csv. Cross-reference account names against your backup admin account list to isolate non-admin domain user logons that are suspicious given CVE-2026-44963's low exploitation bar.

Evidence: Preserve the following before any remediation activity: (1) Windows Security Event Log from the Veeam server covering at least 30 days — export via: wevtutil epl Security C:\evidence\security__.evtx. (2) Veeam application log at C:\ProgramData\Veeam\Backup\Logs\ — these logs record job executions and API calls and may show unauthorized job creation or repository access. (3) Sysmon operational log if deployed — Event ID 1 (Process Create) entries with ParentImage matching Veeam service binaries are the primary forensic indicator of successful RCE exploitation for this CVE. (4) Windows Event ID 4688 entries (Process Creation) filtered on parent processes Veeam.Backup.Service.exe and Veeam.Backup.Manager.exe — unexpected child process spawning here is the strongest indicator of CVE-2026-44963 exploitation.

Step 3: Eradication — Apply the Veeam Backup & Replication 12.3.2 patch per KB4743 on all affected backup servers. Validate the installed build number matches the 12.3.2 fixed build post-upgrade. Audit and revoke any domain user accounts granted access to backup server management interfaces beyond operationally required roles. Reference: NIST SI-2 (no mapped control in provided knowledge base for patch management specifically) — CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), NIST AC-2 (Account Management), NIST AC-6 (Least Privilege)

Compensating: Verify the installed Veeam build post-patch via PowerShell: Get-ItemProperty 'HKLM:\SOFTWARE\Veeam\Veeam Backup and Replication' | Select-Object UIVersion — confirm the value matches the 12.3.2 fixed build number documented in KB4743. For account audit with no IAM tooling, run: net localgroup 'Veeam Backup Administrators' and cross-reference against your approved backup admin list; remove any standard domain user accounts with: net localgroup 'Veeam Backup Administrators' DOMAIN\username /delete. Document each removal with timestamp and approving authority.

Evidence: Before patching, capture a registry export of the Veeam installation key to document the pre-patch build: reg export 'HKLM\SOFTWARE\Veeam\Veeam Backup and Replication' C:\evidence\veeam_build_prepatch.reg. Export current Veeam Backup Administrators local group membership and any domain group delegations to the Veeam console. If exploitation occurred prior to patching, the vulnerable DLL or service binary version is forensic evidence of the attack surface — preserve a hash of relevant Veeam service binaries (Get-FileHash 'C:\Program Files\Veeam\Backup and Replication\Backup\Veeam.Backup.Service.exe') before the installer overwrites them.

Step 4: Recovery — After patching, verify backup job integrity by running a test restore from recent backup chains. Confirm no unauthorized scheduled tasks, services, or startup entries were added to backup servers (reference D3-SICA: System Init Config Analysis). Review system files and executables on backup servers for unauthorized modifications (reference D3-SFA: System File Analysis). Monitor Veeam service account activity for 30 days post-remediation. Reference: NIST AU-6, CIS 8.2.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 8.2 (Collect Audit Logs)

Compensating: Enumerate scheduled tasks added during the exposure window: Get-ScheduledTask | Where-Object {$_.Date -gt ''} | Select-Object TaskName, TaskPath, Date | Export-Csv C:\evidence\new_scheduled_tasks.csv. For file integrity on Veeam server binaries, generate SHA-256 hashes of all executables under C:\Program Files\Veeam\ and compare against hashes from a known-good build documented in the KB4743 advisory. Use Sysinternals Autoruns (autoruns -a -c > autoruns_output.csv) to capture all persistence mechanisms — review for entries not present in a baseline snapshot. For backup chain integrity, initiate a Veeam SureBackup job or manual instant VM recovery test to validate that backup data has not been encrypted or corrupted by ransomware pre-positioned through the CVE-2026-44963 access path.

Evidence: Before declaring recovery complete, capture: (1) Full Autoruns output documenting all persistence points on the Veeam server at time of recovery — this detects backdoors installed via the RCE vector. (2) Veeam backup repository catalog integrity — compare repository metadata against known-good state to detect unauthorized deletion or encryption of backup chains, which is the primary ransomware objective when targeting backup infrastructure. (3) Windows Event ID 7045 (New Service Installed) and Event ID 4698 (Scheduled Task Created) from the Security log covering the full exposure window — these are the most likely persistence mechanisms dropped via CVE-2026-44963 RCE.

Step 5: Post-Incident — Review whether domain user accounts should have any access to backup management infrastructure; implement dedicated, non-domain backup admin accounts where architecture permits. Enforce MFA on all backup server administrative access (CIS 6.5: Require MFA for Administrative Access; D3-MFA: Multi-factor Authentication). Rotate credentials for any service accounts with access to backup infrastructure (D3-CRO: Credential Rotation). Document this gap against NIST AC-6 (Least Privilege) and AC-5 (Separation of Duties) and include in the next risk assessment cycle.

NIST Phase: Post Incident

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

Controls: NIST AC-5 (Separation Of Duties), NIST AC-6 (Least Privilege), NIST AC-2 (Account Management), CIS 6.5 (Require MFA for Administrative Access), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For MFA without enterprise tooling, configure Windows Hello for Business or enable smart card requirements for the Veeam console login via local Group Policy (Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options: 'Interactive logon: Require smart card'). For service account credential rotation on Veeam, update credentials in Veeam console under Backup Infrastructure > Managed Servers > Credentials, and immediately rotate the corresponding AD account password: Set-ADAccountPassword -Identity -Reset -NewPassword (ConvertTo-SecureString -AsPlainText '' -Force). Document all rotated accounts and timestamps.

Evidence: For the lessons-learned record, compile: (1) The complete timeline of domain user logons to the Veeam server during the exposure window (from the Event ID 4624 export captured in Step 2) — this quantifies the actual attack surface exposed by CVE-2026-44963's low authentication bar. (2) A list of all service accounts with credentials stored in Veeam (exported from Veeam console Credentials Manager) that existed at time of incident — any of these could have been harvested if RCE was achieved. (3) The pre-remediation Veeam role assignment export showing which domain users had console access — this is the direct evidence for the AC-6 and AC-5 gap documentation.

Detection Guidance

Primary detection surface is authentication and process telemetry on Veeam Backup & Replication servers. Query Windows Security logs for Event ID 4624 (successful logon) filtering on logon types 3 (network) and 10 (remote interactive) where the account is not a designated backup administrator. Look for Event ID 4688 (process creation) showing unusual child processes spawned under Veeam service executables (e.g., Veeam.Backup.Service.exe, Veeam.Backup.Manager.exe, Veeam.Backup.Shell.exe). In EDR telemetry, hunt for command shell or scripting engine invocations (cmd.exe, powershell.exe, wscript.exe) parented to Veeam processes. Flag any new scheduled tasks, services, or autorun entries created on backup servers (Windows Event IDs 4698, 7045). Per MITRE T1570, look for large or unexpected file writes to backup repositories from non-backup processes. Reference: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-3 (Content of Audit Records), CIS 8.2 (Collect Audit Logs). No confirmed IOCs (IP, domain, hash) are available in the source data for this CVE at this time.

Framework Mappings

MITRE-ATTACK

- **T1210** — Exploitation of Remote Services
- **T1078.002** — Domain Accounts
- **T1570** — Lateral Tool Transfer

NIST-800-53R5

- **AC-6** — Least Privilege
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-10** — Information Input Validation
- **SI-7** — Software, Firmware, and Information Integrity
- **CP-9** — System Backup
- **IR-4** — Incident Handling
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

- **A03:2021** — Injection
- **A01:2021** — Broken Access Control

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts
- **6.8** — Define and Maintain Role-Based Access Control

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **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

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.8.8** — Management of technical vulnerabilities

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1210	Exploitation of Remote Services	Lateral-Movement
T1078.002	Domain Accounts	Defense-Evasion
T1570	Lateral Tool Transfer	Lateral-Movement

Sources

Source	URL	Tier
	https://thehackernews.com/2026/06/veeam-backup-replication-rce-flaw...	T3
Veeam Backup & Replication RCE Flaw Lets Domain Users Run ...	https://x.com/TheCyberSecHub/status/2064409843646242816	T3
Vulnerabilities Resolved in Veeam Backup & Replication 12.3.2	https://www.veeam.com/kb4743	T3
New Veeam RCE flaw lets domain users hack backup servers	https://www.linkedin.com/posts/gvarisco_new-veeam-rce-flaw-lets-dom...	T3
Critical Veeam RCE flaw Lets Low-Privilege Users Take Over ...	https://securityaffairs.com/193385/uncategorized/critical-veeam-rce...	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-44963	T1

Generated 2026-06-10 07:26 UTC by TJS Security Command Center