INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:37 UTC

Veeam Patches 7 Critical Backup & Replication Flaws Allowing Remote Code Execution

SECURITY ANALYSIS | CRITICAL | CVSS 9.8

SCC Item ID	SCC-CVE-2026-0010
Type	Security Analysis
Severity	CRITICAL
CVSS Base Score	9.8
Affected Products	Veeam Backup & Replication (fixed in version 12.3.2.4465)
Published	1 day ago
Discovery Source	Rss

Executive Summary

Veeam released patches in March 2026 for seven critical vulnerabilities in Backup & Replication software, all carrying a CVSS base score of 9.8, that allow unauthenticated remote code execution against backup servers. Organizations running Veeam Backup & Replication below version 12.3.2.4465 are exposed. Ransomware operators routinely target backup infrastructure to eliminate recovery options before detonating payloads, making unpatched backup servers a direct threat to business continuity. Verify specific CVE identifiers and affected version ranges in Veeam KB4830 before deployment.

Technical Analysis

Veeam Backup & Replication versions prior to 12.3.2.4465 contain seven critical-rated vulnerabilities enabling remote code execution. CVSS base scores are reported at 9.8, indicating network-accessible attack vectors requiring no authentication and no user interaction. MITRE ATT&CK mapping covers T1133 (External Remote Services), T1210 (Exploitation of Remote Services), and T1486 (Data Encrypted for Impact), consistent with ransomware pre-positioning behavior targeting backup infrastructure. Specific CVE identifiers and CWE classifications were not included in the source data at time of publication; consult Veeam KB4830 directly for the full vulnerability list and technical exploit details. The fixed version is 12.3.2.4465. Veeam's official remediation guidance is published at https://www.veeam.com/kb4830 (verify URL resolves to current KB content before acting). Note: EPSS scores and KEV status were not available in the source data at time of publication.

Action Checklist

1. Step 1, Patch immediately: Upgrade all Veeam Backup & Replication instances to version 12.3.2.4465 per Veeam KB4830 (https://www.veeam.com/kb4830). Consult vendor guidance for patch delivery and compatibility. Prioritize internet-facing or externally reachable backup servers first.
2. Step 2, Restrict network access: Until patching is complete, apply firewall rules or network segmentation to limit inbound access to Veeam backup server ports (default TCP 9392, 9401, 9419) to authorized management hosts only.
3. Step 3, Inventory exposure: Identify all Veeam Backup & Replication deployments across the environment, including versions and network exposure. Flag any instances reachable from untrusted networks or the internet.
4. Step 4, Audit recent activity: Review Veeam server logs for anomalous authentication attempts, unexpected process execution, or unusual outbound connections in the period preceding patch application. Cross-reference with SIEM alerts.
5. Step 5, Communicate and review controls: Notify IT leadership and relevant stakeholders of patch status. Review backup server access controls, least-privilege configurations, and network segmentation policies to reduce future attack surface.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to C-level management and external IR firm immediately if any evidence of successful exploitation is found (unexpected process execution, lateral movement, data exfiltration, or unauthorized account creation within 30 days preceding patch), or if backup server is internet-facing and has not been patched within 72 hours of advisory publication.
Recovery Notes	Post-containment: Verify backup integrity by running consistency checks on all backup jobs (Veeam console > Backup Infrastructure > Repositories > right-click > Verify Backup Files) and execute test restores of critical datasets to ensure ransomware did not corrupt backup chains. Re-enable automated backup jobs and monitor job completion logs daily for 14 days. Conduct post-incident review with IT leadership to document lessons learned and update incident response playbooks with Veeam-specific detection signatures (scan logs for process execution anomalies matching exploitation patterns documented in Veeam KB4830).

Forensic Artifacts	Veeam application logs: C:\ProgramData\Veeam\Logs\BackupServer.log, Service.log, Tracer.log (30-day lookback; parse for ERROR/WARN, authentication failures, RCE indicators) | Windows Security Event Log: Event IDs 4624 (successful logon), 4625 (failed logon), 4688 (process creation), 4720 (user account created), 4733 (user added to group) — focus on unexpected service account activity and administrative privilege grants | Windows Sysmon logs (if deployed): Event ID 3 (Network Connection), Event ID 1 (Process Creation), Event ID 7 (Image Loaded) — correlate to TCP ports 9392/9401/9419 and unexpected child processes spawned by Veeam services | Veeam database transaction logs: Default SQL Express instance (VEEAMSQL2012) backup database job execution history, job failure logs, and data restore transaction records — check for unauthorized job modifications or deletions | Network artifacts: tcpdump/PCAP from backup server gateway interface (ports 9392/9401/9419), DNS query logs for Veeam server hostname (check for external resolution), and firewall logs showing inbound connection attempts from untrusted sources within 30 days pre-patch

Per-Action IR Details

Step 1, Patch immediately: Upgrade all Veeam Backup & Replication instances to version 12.3.2.4465 per Veeam KB4830 (https://www.veeam.com/kb4830). Consult vendor guidance for patch delivery and compatibility. Prioritize internet-facing or externally reachable backup servers first.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation phase — vulnerability management and patch deployment)

Controls: NIST 800-53 SI-2 (Flaw Remediation), NIST 800-53 SI-2(2) (Automated Flaw Remediation Monitoring), CIS 3.10 (Address Unauthorized Software)

Compensating: Offline patching: Download patch binary from Veeam KB4830 on isolated workstation, transport via USB to air-gapped backup server, execute installer with local admin credentials and verbose logging. Log command: 'msiexec.exe /i VeeamBackupReplication_12.3.2.4465.msi /l*v C:\ProgramData\Veeam\patch_install.log'. Verify post-patch version via Veeam console (Help > About) or PowerShell: 'Get-VBRVersion'.

Evidence: Capture pre-patch baseline: Export Veeam backup job configuration and job history via Veeam console (File > Export Configuration), record current installed version via registry HKLM\Software\Veeam\Veeam Backup and Replication (key: InstallationPath, ProductVersion), export Windows Update history (Get-HotFix), and preserve Veeam installer logs from C:\ProgramData\Veeam\Logs\Install before patch execution.

Step 2, Restrict network access: Until patching is complete, apply firewall rules or network segmentation to limit inbound access to Veeam backup server ports (default TCP 9392, 9401, 9419) to authorized management hosts only.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.2.4 (Containment strategy — network segmentation and access restriction)

Controls: NIST 800-53 AC-3 (Access Enforcement), NIST 800-53 SC-7 (Boundary Protection), CIS 3.12 (Configure Data Access Control), CIS 4.1 (Establish and Maintain a Firewall Configuration Standard)

Compensating: On Windows Firewall: Run 'netsh advfirewall firewall add rule name="Block_Veeam_RCE_Exposure" dir=in action=block protocol=tcp localport=9392,9401,9419 remoteip=!' (e.g., remoteip=!192.168.1.0/24). On Linux iptables: 'iptables -A INPUT -p tcp --dport 9392:9419 ! -s -j DROP && iptables-save > /etc/iptables/rules.v4'. Document rule creation timestamps and test connectivity from authorized host only.

Evidence: Snapshot current firewall configuration before rule insertion: Export Windows Firewall rules (Get-NetFirewallRule -Enabled $true | Export-Csv firewall_baseline.csv), export iptables rules (iptables-save > iptables_baseline.txt), and capture network interface configuration (ipconfig /all on Windows, ip addr show on Linux) to establish baseline for later forensic comparison if breach is suspected.

Step 3, Inventory exposure: Identify all Veeam Backup & Replication deployments across the environment, including versions and network exposure. Flag any instances reachable from untrusted networks or the internet.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.1 (Detection and Analysis — asset inventory and exposure assessment)

Controls: NIST 800-53 CA-7 (Continuous Monitoring), NIST 800-53 CM-8 (Information System Component Inventory), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Manual PowerShell discovery: 'Get-WmiObject Win32_Product -Filter "Name LIKE '%Veeam Backup%'" | Select-Object Version, InstallLocation' across network subnets via remote WMI queries. Use nmap for external port scanning: 'nmap -p 9392,9401,9419 -oA veeam_exposure_scan' to identify externally reachable instances. Cross-reference Active Directory: 'Get-ADComputer -Filter {OperatingSystem -like "*Server*"} | Select-Object Name, DNSHostName' and correlate with patch status via manual version checks or WSUS logs (C:\Program Files\Update Services\LogFiles\SoftwareDistribution.log).

Evidence: Before inventory, establish baseline network capture: tcpdump on backup server gateway ('tcpdump -i eth0 -w veeam_traffic_baseline.pcap port 9392 or 9401 or 9419 -G 3600') to record normal inbound connection patterns. Document current network topology diagram (VLANs, DMZ placement, route tables). Capture Veeam server bindings via netstat: 'netstat -ano | findstr :9392' or 'ss -tlnp | grep -E "9392|9401|9419"'. Export DNS resolution logs from DNS server for Veeam server hostname to detect any unauthorized external queries.

Step 4, Audit recent activity: Review Veeam server logs for anomalous authentication attempts, unexpected process execution, or unusual outbound connections in the period preceding patch application. Cross-reference with SIEM alerts.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.1.4 (Determine whether an incident has occurred — log analysis and anomaly detection)

Controls: NIST 800-53 AU-2 (Audit Events), NIST 800-53 SI-4 (Information System Monitoring), CIS 8.2 (Collect Audit Logs), CIS 8.5 (Implement Automated Alerts on Account Usage)

Compensating: Veeam log analysis: Parse Veeam trace logs (C:\ProgramData\Veeam\Logs\BackupServer.log, C:\ProgramData\Veeam\Logs\Service.log) for ERROR and WARN entries in last 30 days using PowerShell: 'Select-String -Path 'C:\ProgramData\Veeam\Logs*.log' -Pattern "(ERROR|authentication|unauthorized|RCE)" | Export-Csv veeam_anomalies.csv'. Windows Event Log analysis: Query event ID 4688 (Process Creation) and 4720 (User Account Created) on backup server: 'Get-WinEvent -FilterHashtable @{LogName="Security"; ID=4688,4720; StartTime=(Get-Date).AddDays(-30)} | Where-Object {$_.Message -match "veeam|backup|cmd|powershell|rundll32"} | Export-Csv process_audit.csv'. Network: Use netstat historical logs or Sysmon (if deployed): 'Get-WinEvent -FilterHashtable @{LogName="Sysmon"; ID=3; StartTime=(Get-Date).AddDays(-30)} | Where-Object {$_.Message -match "9392|9401|9419" -and $_.Message -notmatch ""} | Export-Csv outbound_connections.csv'.

Evidence: Preserve Veeam application logs before any cleanup: Copy C:\ProgramData\Veeam\Logs* to forensic storage with timestamps intact (robocopy C:\ProgramData\Veeam\Logs E:\Forensics\Veeam_PrePatch_Logs /MIR /COPY:DAT). Export Windows Security event log to EVT file for 30-day lookback: 'wevtutil epl Security E:\Forensics\Security_30day.evtx /overwrite:true' (filter to events 4624, 4625, 4688, 4720, 4733). Capture Veeam database transaction logs if SQL-backed (typically SQL Express, default instance VEEAMSQL2012): 'BACKUP LOG [VeeamBackupDB] TO DISK = 'E:\Forensics\VeeamBackupDB_txn.bak' WITH NOFORMAT, NOINIT'. Export network connection history via Get-NetTCPConnection: 'Get-NetTCPConnection -State Established | Where-Object {$_.LocalPort -match "9392|9401|9419"} | Export-Csv active_connections.csv'.

Step 5, Communicate and review controls: Notify IT leadership and relevant stakeholders of patch status. Review backup server access controls, least-privilege configurations, and network segmentation policies to reduce future attack surface.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4.1 (Post-Incident Activities — lessons learned and control hardening)

Controls: NIST 800-53 AC-2 (Account Management), NIST 800-53 AC-6 (Least Privilege), NIST 800-53 CA-7 (Continuous Monitoring), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.2 (Ensure Proper User Access Management)

Compensating: Access control audit: Query Veeam local administrators via 'Get-LocalGroupMember -Group "Administrators" | Export-Csv veeam_admins.csv' and correlate to Active Directory: 'Get-ADGroupMember -Identity "" | Export-Csv ad_veeam_admins.csv'. Review NTFS permissions on Veeam installation and data directories: 'icacls C:\Program Files\Veeam /T /C > veeam_install_perms.txt' and 'icacls C:\ProgramData\Veeam /T /C > veeam_data_perms.txt'. Validate least-privilege service account used by Veeam backup server: 'Get-WmiObject Win32_Service -Filter "Name LIKE '%Veeam%'" | Select-Object Name, StartName, State'. Generate change log for next 90 days to monitor for unauthorized modifications: Configure File Integrity Monitoring on C:\Program Files\Veeam* and C:\ProgramData\Veeam* (use Sysmon FileCreate/FileDelete events or Windows auditing: 'auditpol /set /subcategory:"File System" /success:enable /failure:enable').

Evidence: Baseline access controls pre-hardening: Export current NTFS ACLs, local group memberships, and AD group memberships before any removal of accounts or permissions. Capture Veeam service account permissions: 'Get-WmiObject Win32_LogicalFileSecuritySetting -Path 'C:\ProgramData\Veeam' -ErrorAction SilentlyContinue | Invoke-WmiMethod -Name GetSecurityDescriptor | Select-Object -ExpandProperty Descriptor | Export-Csv veeam_data_secdesc.csv'. Document pre-hardening network segmentation: Export firewall rules, VLAN assignments, and routing tables. Create a snapshot of current Group Policy Objects (GPOs) affecting backup servers: 'Get-GPO -All | Export-Csv gpo_snapshot.csv' and link audit events: 'Get-WinEvent -FilterHashtable @{LogName="Directory Service"; EventID=5136; StartTime=(Get-Date).AddDays(-7)} | Export-Csv gpo_audit.csv'.

Detection Guidance

Focus detection on the Veeam backup server host and its network traffic. Key indicators to investigate: (1) Unexpected processes spawned by Veeam service accounts (VeeamBackupSvc, VeeamTransportSvc), look for cmd.exe, powershell.exe, or scripting engine child processes in Windows Security and Sysmon Event ID 1 logs. (2) Inbound connections to Veeam management ports (TCP 9392, 9401, 9419) from IP addresses outside authorized management ranges, check firewall and netflow logs. (3) New scheduled tasks, registry run keys, or service installations on the backup server following external connection events. (4) Volume shadow copy deletion commands (vssadmin delete shadows, wmic shadowcopy delete) on systems the backup server communicates with, which may indicate ransomware staging. (5) Outbound connections from the backup server to uncommon external IPs or known threat infrastructure. Note: Specific CVE identifiers and exploit-specific IOCs were not available in the source data at time of publication; monitor Veeam KB4830 and threat intelligence feeds for updated indicators as exploitation details are published.

Framework Mappings

MITRE-ATTACK

- **T1133** — External Remote Services
- **T1210** — Exploitation of Remote Services
- **T1486** — Data Encrypted for Impact

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
- **AC-6** — Least Privilege
- **SI-2** — Flaw Remediation
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **IR-4** — Incident Handling

NIST-CSF-2

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

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
- **A.5.23** — Information security for use of cloud services

CIS-V8

- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1133	External Remote Services	Persistence
T1210	Exploitation of Remote Services	Lateral-Movement
T1486	Data Encrypted for Impact	Impact

Sources

Source	URL	Tier
The Hacker News	https://thehackernews.com/2026/03/veeam-patches-7-critical-backup.html	T3
Vulnerabilities Resolved in Veeam Backup & Replication 12.3.2.4465	https://www.veeam.com/kb4830	T3
Veeam warns of critical flaws exposing backup servers to RCE attacks	https://www.bleepingcomputer.com/news/security/veeam-warns-of-criti...	T3

Source	URL	Tier
Veeam Patches 7 Critical Backup & Replication Flaws Allowing ...	https://www.reddit.com/r/SecOpsDaily/comments/1rsfcxj/veeam_patches...	T3
Veeam warns admins to patch now as critical RCE flaws hit Backup ...	https://www.csoonline.com/article/4144882/veeam-warns-admins-to-pat...	T3
Veeam issues patch to close critical remote code execution flaw	https://cyberscoop.com/veeam-backup-replication-security-flaw-remot...	T3
Several Code Execution Flaws Patched in Veeam Backup ...	https://www.securityweek.com/several-code-execution-flaws-patched-i...	T3
Vulnerabilities Resolved in Veeam Backup & Replication 13.0.1.1071	https://www.veeam.com/kb4792	T3
New Veeam vulnerabilities expose backup servers to RCE attacks	https://www.bleepingcomputer.com/news/security/new-veeam-vulnerabil...	T3

Generated 2026-03-29 18:37 UTC by TJS Security Command Center