ultraviolet

THREAT ADVISORY

VM Replication Tool Threats

Services Performed By:
UltraViolet Cyber TIDE Team
tide@uvcyber.com

Published Date:
June 10, 2026
TLP:GREEN

Executive Snapshot

Veeam Backup and Replication, one of the most widely deployed enterprise data protection platforms globally, has disclosed a critical remote code execution vulnerability tracked as CVE-2026-44963, carrying a CVSS score of 9.4. The flaw allows any authenticated domain user to execute arbitrary code on the backup server, a low privilege bar that exposes virtually every domain-joined deployment to potential full system compromise. Veeam patched the vulnerability in build 12.3.2.4854 on June 9, 2026, but history strongly suggests that unpatched organizations face imminent exploit attempts: prior Veeam vulnerabilities including CVE-2024-40711 were weaponized by Akira and Fog ransomware groups within weeks of public disclosure, and Rapid7 reported that Veeam featured in more than 20 percent of its incident response engagements in 2024. This is not a Veeam-specific problem, Commvault, NAKIVO, and other replication tools have each disclosed critical RCE and path traversal vulnerabilities in the past 18 months, several of which were exploited by nation-state actors and ransomware groups before patches were widely applied. The pattern is consistent: threat actors target backup infrastructure first because eliminating recovery options maximizes ransomware leverage.

- Apply the CVE-2026-44963 patch immediately by upgrading all domain-joined Veeam deployments to build 12.3.2.4854, and audit all other backup and replication platforms including Commvault and NAKIVO against their respective current patch levels.

- Isolate backup infrastructure from general network access by enforcing strict network segmentation, restricting management interfaces to known administrative hosts, and removing any internet-facing exposure of backup consoles or APIs.

- Enforce multi-factor authentication on all access pathways into backup environments, including VPN gateways, remote desktop sessions, and backup management consoles, to eliminate the risk of compromised domain credentials being used to trigger RCE.

TIDE Team Analysis

The latest critical vulnerability disclosed in Veeam Backup and Replication, tracked as CVE-2026-44963, represents not an isolated incident but a continuation of a deeply concerning pattern across the enterprise backup and replication industry. The flaw carries a CVSS score of 9.4 and enables any authenticated domain user to execute arbitrary remote code directly on the backup server. Discovered by WatchTowr researcher Sina Kheirkhah, the vulnerability has a notably low privilege requirement that dramatically widens the attack surface, affecting domain-joined Veeam deployments running version 12.x up to and including build 12.3.2.4465. Veeam released a patch in version 12.3.2.4854 on June 9, 2026, and organizations running earlier builds should treat themselves as actively at risk until the update is applied.

This is not theoretical caution; it is a documented behavioral pattern that Veeam itself has acknowledged: once a patch is publicly disclosed, threat actors routinely reverse-engineer the fix to develop exploits targeting unpatched systems. The broader context of this disclosure is a string of critical findings across Veeam's product line throughout 2025 and into 2026. In October 2025, CERT-EU issued an advisory covering two additional Veeam flaws, CVE-2025-48983 and CVE-2025-48984, both carrying CVSS scores of 9.9, allowing authenticated domain users to execute arbitrary code on backup infrastructure hosts and the backup server respectively. Earlier in January 2026, Veeam patched CVE-2025-59470, a CVSS 9.0 flaw allowing a backup or tape operator to perform remote code execution as the PostgreSQL database user. In March 2026, Veeam patched a further cluster of critical flaws including CVE-2026-21666, CVE-2026-21667, and CVE-2026-21708, each carrying a CVSS score of 9.9, with the latter allowing an attacker holding only Backup Viewer permissions to execute code as the internal database user.

The exploitation history for Veeam vulnerabilities is extensive and involves multiple ransomware groups operating at scale. In September 2024, Veeam disclosed CVE-2024-40711, a critical unauthenticated RCE flaw with a CVSS score of 9.8. Sophos tracked a series of attacks in which threat actors accessed targets through compromised VPN gateways lacking multi-factor authentication, exploited the vulnerability to spawn local administrator accounts, and deployed ransomware, with confirmed attacks linked to both Akira and Fog ransomware variants. Earlier Veeam vulnerabilities, including CVE-2023-27532, had already been exploited by ransomware groups including EstateRansomware, Akira, Cuba, and FIN7 for initial access, credential theft, and lateral movement. Rapid7 noted that more than 20 percent of its incident response cases in 2024 involved Veeam being accessed or exploited in some manner, typically after an adversary had already established a foothold in the environment.

The problem is industry-wide and not confined to a single vendor. Commvault, a widely deployed alternative, has been subjected to sustained and escalating vulnerability research. CVE-2025-34028, a path traversal vulnerability in Commvault Command Center, received the maximum CVSS severity score of 10.0 and was added to CISA's Known Exploited Vulnerabilities catalog after a proof-of-concept exploit was published. A separate Commvault flaw, CVE-2025-3928, was exploited in zero-day attacks by a nation-state threat actor before it was patched. WatchTowr subsequently returned to Commvault and uncovered four additional weaknesses, including CVE-2025-57789, which allowed attackers to decrypt a built-in administrator password using a hard-coded key, and CVE-2025-57790, a path traversal issue enabling attackers to drop a web shell and execute arbitrary commands, vulnerabilities that could be combined into two separate pre-authentication RCE chains.

NAKIVO Backup and Replication, deployed widely among managed service providers and mid-market enterprises, has also come under direct attack. CVE-2024-48248 is an absolute path traversal vulnerability allowing remote, unauthenticated attackers to read files from the affected system, exposing configuration files, backup contents, and stored credentials. CISA added it to the Known Exploited Vulnerabilities catalog after active exploitation was confirmed. The credential exposure dimension is especially significant: backup and replication platforms routinely

store privileged credentials for large portions of the environment they protect, meaning a successful compromise of the backup server is effectively equivalent to obtaining a master key for the infrastructure it touches.
The strategic logic driving ransomware operators toward backup infrastructure is straightforward and well understood within the threat intelligence community. Backup systems represent the organization's last line of defense against a ransomware event. An adversary who compromises backup infrastructure before deploying encryption removes the victim's ability to recover independently, dramatically increasing ransom leverage and enabling double-extortion scenarios. CISA has flagged four separate Veeam Backup and Replication flaws as actively exploited in attacks, all abused by ransomware gangs. The frequency with which researchers at WatchTowr, Sophos, and Rapid7 are finding and observing exploitation of these vulnerabilities confirms that the attacker community has concluded backup platforms are high-return, under-hardened targets.

From an architectural risk perspective, the CVE-2026-44963 disclosure introduces a nuance that organizations should assess carefully. The vulnerability only affects domain-joined Veeam installations, meaning organizations running Veeam in a workgroup configuration rather than an Active Directory domain environment are not impacted by this specific flaw. However, the overwhelming majority of enterprise deployments are domain-joined, and the low privilege requirement, a standard authenticated domain user account, means the effective attack surface is any user credential in the environment. Veeam has confirmed the vulnerability does not affect version 13.x builds due to architectural changes introduced in that release, which underscores that organizations should treat the upgrade path to version 13 as a longer-term strategic priority rather than treating the current patch as a final resolution.

The executive recommendation is that backup and replication infrastructure be reclassified within the organization's threat model from a data protection asset to a Tier 1 critical system subject to the same controls applied to identity infrastructure and production systems. Immediate priorities include applying the CVE-2026-44963 patch, auditing all Veeam and competing platforms for outstanding CVEs, enforcing network segmentation that limits access to backup servers to known management hosts only, eliminating internet-exposed backup management interfaces, and requiring multi-factor authentication on all pathways into these environments. Third-party platforms including Commvault and NAKIVO should be subjected to the same patch review cycle. Organizations without a tested incident response playbook specific to backup infrastructure compromise should treat that as a critical gap, given how consistently these systems now appear in the pre-encryption phase of ransomware intrusions.

Why It Matters

The targeting of backup and replication infrastructure by ransomware groups and nation-state actors is not a recent development; it is a deliberate, sustained, and increasingly sophisticated campaign that has been building for several years. The foundational logic is simple: an organization with intact backups is far less likely to pay a ransom, so adversaries have learned to eliminate that option before deploying encryption. This calculus shifted the threat landscape materially around 2022 and 2023, when ransomware groups began treating backup servers not as secondary targets but as primary objectives in the early stages of an intrusion. The EstateRansomware, Cuba, and FIN7 groups were among the first to operationalize this approach at scale, exploiting CVE-2023-27532 in Veeam Backup and Replication to gain initial access, harvest credentials, and move laterally before their presence was detected. That single vulnerability established a template that threat actors have returned to repeatedly, refining their techniques with each new disclosure.

The period between 2024 and 2025 marked a significant escalation in both the volume and severity of vulnerabilities discovered across the backup platform industry. Veeam's CVE-2024-40711, a critical unauthenticated RCE flaw rated 9.8, became one of the most actively exploited enterprise vulnerabilities of 2024, linked to confirmed attacks by Akira, Fog, and Frag ransomware variants. Commvault suffered a nation-state zero-day exploitation of CVE-2025-3928 before a patch was even available, and subsequently disclosed CVE-2025-34028, a maximum-severity path traversal flaw that enabled unauthenticated remote code execution and was added to CISA's Known Exploited Vulnerabilities catalog within weeks of its proof-of-concept publication. NAKIVO's CVE-2024-48248 followed a similar arc, moving from researcher disclosure to confirmed active exploitation before many organizations had completed their patch cycle. What unified these incidents was not simply their severity but the speed at which they were operationalized; the window between public disclosure and active exploitation had collapsed from months to days.

A critical and underappreciated dimension of this threat is the privileged position that backup and replication platforms occupy within enterprise environments. These systems are not passive data stores; they are deeply integrated, highly privileged components that maintain credentials for every system they protect, communicate with hypervisors, storage arrays, and cloud endpoints, and in many deployments operate with domain administrator-equivalent access. When WatchTowr researchers documented their findings across Veeam, Commvault, and NAKIVO, they consistently highlighted that the real prize was not the backup data itself but the credential stores and integration tokens that these platforms accumulate over time. A single compromised backup server can provide an adversary with the lateral movement capability to reach production systems, domain controllers, and cloud tenants, effectively converting a targeted attack on one platform into a full enterprise compromise.

The trend line points in one direction. The research community's sustained focus on backup and replication tools has not deterred attackers; it has accelerated a race between defenders patching and adversaries operationalizing exploits. CISA has now catalogued multiple backup platform vulnerabilities as actively exploited in the wild, NHS England has issued specific advisories warning that enterprise backup applications are high-value targets for cyber threat groups, and incident response data consistently shows these platforms appearing in the pre-encryption phase of ransomware intrusions. For CTOs and CISOs, the historical record makes clear that backup infrastructure must be treated as attack surface, not safety net. Organizations that continue to apply lower security standards to backup systems than to production systems, relaxed patching cadences, weaker access controls, limited monitoring, are making a strategic error that threat actors are actively counting on.

How to Respond

- Strictly adhere to cybersecurity Fundamentals and ensure all personnel undergo annual phishing and social engineering training. Speak with your UltraViolet Cyber TAM Representative to schedule a live phishing engagement.
- Ensure all VM replication and backup tools are updated per vendors specifications.
- Perform annual tech refresh reviews to gain a holistic understanding of your infrastructure. Speak with your UltraViolet Cyber TAM Representative to schedule a RedTeam or PurpleTeam engagement to gain insight into the vulnerabilities in your environment.

What UltraViolet Cyber is Doing

- Tracking new CVEs and high impact vulnerabilities, analyzing and deploying public Proof-Of-Concept code against custom built targets.
- Proactively enabling custom detections based on the collected artifacts, tactics, techniques, and procedures identified in this activity.
- Performing hypothesis driven threat hunts based on threat actor behavior and artifacts. UVCyber customers will be informed of the results through secure channels.
- Parsing available victim dump data for any social, financial, business, or technical relations to UVCyber Clients and partner organizations.
- Aggregating threat intelligence from myriad sources and applying the most up-to-date knowledge to proactive threat hunting and response.

About UltraViolet Cyber

UltraViolet Cyber is a leading tech-enabled managed security services provider, delivering unparalleled cybersecurity expertise that fills technology and talent gaps across Global 2000 and Federal Government customers. Founded and operated by security practitioners from the national intelligence community, UltraViolet Cyber connects offensive security, application security, detection and response, and security engineering to deliver a differentiated approach to cybersecurity operations. Transforming customers' security programs, UltraViolet Cyber's flagship security-as-a-service solution, UV Lens, removes complex operational silos, replacing them with integrated security capabilities. UltraViolet is headquartered in McLean, Virginia with technology centers across the world.

443.351.7630 / info@uvcyber.com | UltraViolet Cyber | @uv_cyber

---