INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-10 15:52 UTC

UNVERIFIED: Azure HorizonDB Unauthenticated Authentication Bypass, CVE-2026-48567

CVE VULNERABILITY | **CRITICAL** | CVSS 10.0

SCC Item ID	SCC-CVE-2026-0290
Type	CVE Vulnerability
CVE ID	CVE-2026-48567
Severity	CRITICAL
CVSS Base Score	10.0
EPSS Score	0.0010 (27th percentile)
Affected Products	Azure HorizonDB (version unconfirmed, source unverified)
Published	2026-06-08
Discovery Source	Gemini

Executive Summary

INTEGRITY NOTICE: CVE-2026-48567, claimed as a critical authentication bypass in 'Azure HorizonDB,' could not be verified against NVD, CISA KEV, or Microsoft official advisory channels. The product 'Azure HorizonDB' does not appear in Microsoft's published Azure service catalog. Validate this CVE independently against NVD (nvd.nist.gov) and Microsoft Security Response Center (msrc.microsoft.com) before taking any organizational action. All technical details below are sourced from unconfirmed input and must not be relied upon without authoritative corroboration.

Technical Analysis

UNVERIFIED, treat as unconfirmed until independently validated against NVD and MSRC. Raw input claims CVE-2026-48567 is an authentication bypass in a product called 'Azure HorizonDB,' with a reported CVSS 10.0 and network-based attack vector requiring no privileges or user interaction. The claimed impact is unauthorized access without authentication. Affected version range is unconfirmed. No CWE identifiers are available; if confirmed, likely candidates include CWE-287 (Improper Authentication) and CWE-306 (Missing Authentication for Critical Function). No MITRE ATT&CK techniques are confirmed; if validated, likely mappings include T1078 (Valid Accounts) and T1556 (Modify Authentication Process). CVSS vector string is not provided; severity cannot be independently validated. The product 'Azure HorizonDB' does not appear in publicly indexed Microsoft Azure service documentation as of 2026-03-04. EPSS score of 0.00098 (26.9th percentile) is inconsistent with claimed critical severity and suggests minimal observed exploitation, a further integrity signal

warranting verification. No vendor advisory, patch, or Microsoft Security Update Guide entry has been confirmed from authoritative sources. Source quality assessment is uncertain; the T1 NVD URL has not been confirmed as resolving to valid content.

Action Checklist

1. Step 1: Validate Before Acting, Before any containment action, confirm this CVE exists by checking NVD directly at nvd.nist.gov and Microsoft Security Response Center (MSRC) at msrc.microsoft.com. Do not treat this item as confirmed until an authoritative source resolves the CVE. If confirmed, proceed to Step 2.
2. Step 2: Containment (if confirmed), Identify any instances of the affected product in your environment using asset inventory controls (NIST SI-4 system monitoring; CIS 1.1 asset inventory). Isolate internet-facing instances behind network controls. Restrict access to trusted IP ranges pending official patch confirmation.
3. Step 3: Detection (if confirmed), Query authentication logs for anomalous privilege escalation events originating from unauthenticated or invalid sessions. No specific IOC patterns are confirmed from authoritative sources; monitor for zero-authentication request patterns and authentication failures followed by successful privilege escalation (NIST AU-6 audit record review; CIS 8.2 audit log collection).
4. Step 4: Eradication (if confirmed), Apply the vendor-issued patch once a verified Microsoft advisory is published. No patch ID or version upgrade path is confirmed from unverified sources; do not apply third-party guidance without Microsoft MSRC corroboration. Confirm remediation against the official MSRC advisory.
5. Step 5: Post-Incident, If this CVE confirms as valid, review asset inventory completeness (CIS 1.1), ensure all Azure-hosted database services are enumerated and version-tracked, and verify that unverified intelligence items in your pipeline are held for source validation before driving operational response. Recommendation: implement a formal intelligence triage gate (per NIST RA-3 risk assessment) to prevent unverified critical items from auto-escalating.

Detection Guidance

UNVERIFIED ITEM, no confirmed IOCs, attack signatures, or behavioral indicators are available from authoritative sources. If this vulnerability is confirmed: monitor authentication logs on the affected product for requests that succeed without valid credential presentation; alert on privilege-level changes in sessions originating from unauthenticated or invalid authentication states; review network logs for unexpected inbound connections from external IPs. Per NIST AU-6, audit records should be reviewed for authentication anomalies. Per CIS 8.2, ensure audit logging is active and monitored on all database services in your environment. Until NVD or Microsoft MSRC confirms the CVE, any detection rule written for this vulnerability should be treated as hypothetical and held in draft status.

Framework Mappings

NIST-800-53R5

- **IA-2** — Identification and Authentication (Organizational Users)

- **AC-6** — Least Privilege

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts

HIPAA-SECURITY

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

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures
- **CC6.3** — Authorizes, modifies, or removes access

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.23** — Information security for use of cloud services

Sources

Source	URL	Tier
CVE-2026-48567 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-48567	T1
CVE-2026-48567 | Tenable®	https://www.tenable.com/cve/CVE-2026-48567	T3
Critical Authentication Bypass in Azure HorizonDB (CVE-2026-48567)	https://www.thehackerwire.com/critical-authentication-bypass-in-azu...	T3
Azure HorizonDB Authentication Bypass (CVE-2026-48567)	https://threat-modeling.com/azure-horizondb-auth-bypass-cve-2026-48...	T3
CVE-2026-46067: Linux Kernel Buffer Overflow Vulnerability	https://www.sentinelone.com/vulnerability-database/cve-2026-46067/	T3

Generated 2026-06-10 15:52 UTC by TJS Security Command Center