INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-15 06:40 UTC

CVE-2026-34182: CMS AuthEnvelopedData Forgery Vulnerability in Microsoft Azure Linux cloud-hypervisor

CVE VULNERABILITY | **CRITICAL** | CVSS 9.1

SCC Item ID	SCC-CVE-2026-0300
Type	CVE Vulnerability
CVE ID	CVE-2026-34182
Severity	CRITICAL
CVSS Base Score	9.1
EPSS Score	0.0001 (0th percentile)
Affected Products	Microsoft azl3 cloud-hypervisor 51.1.56-1 on Azure Linux 3.0
Published	2026-06-13T01:43:38
Discovery Source	Msrc Patch Tuesday

Executive Summary

A critical cryptographic integrity flaw in the Azure Linux 3.0 cloud-hypervisor package allows forged CMS AuthEnvelopedData messages to pass authentication checks, carrying a CVSS base score of 9.1. Organizations running Microsoft Azure Linux 3.0 virtual machines on Azure infrastructure with the affected cloud-hypervisor package (azl3 version 51.1.56-1) are at risk of workload isolation compromise and inter-VM communication tampering. Microsoft disclosed this vulnerability as part of the June 2026 Patch Tuesday cycle; patching should be treated as urgent for affected Azure Linux 3.0 deployments.

Technical Analysis

CVE-2026-34182 is a cryptographic integrity failure in CMS (Cryptographic Message Syntax) AuthEnvelopedData processing within the azl3 cloud-hypervisor package version 51.1.56-1 on Azure Linux 3.0. AuthEnvelopedData combines encryption and authenticated encryption (AEAD); the vulnerability stems from improper validation of the authentication tag, mapped to CWE-354 (Improper Validation of Integrity Check Value) and CWE-347 (Improper Verification of Cryptographic Signature). An attacker able to inject or substitute CMS-encapsulated messages in the hypervisor's processing pipeline could bypass integrity verification, causing the hypervisor to accept forged or tampered content as authentic. In a cloud hypervisor context this has implications for VM-to-hypervisor message integrity and potentially workload isolation boundaries. Relevant

MITRE ATT&CK techniques: T1600 (Weaken Encryption) and T1565 (Data Manipulation). CVSS base score: 9.1 (Critical); EPSS score: 0.005% (percentile 0.23%), exploitation is not yet observed in the wild and the CVE is not listed in the CISA KEV catalog as of the data provided. Primary authoritative source: MSRC Update Guide at https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-34182. No exploit code or active threat actor attribution is present in the provided source data.

Action Checklist

1. Step 1: Isolation and Asset Inventory. Identify all Azure Linux 3.0 hosts running cloud-hypervisor package azl3 version 51.1.56-1. Run 'rpm -q cloud-hypervisor' or equivalent on Azure Linux 3.0 nodes to confirm exposure. Isolate high-sensitivity workloads running on affected hypervisor hosts until patching is complete. Reference: MSRC Update Guide for CVE-2026-34182 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-34182).
2. Step 2: Detection. Review hypervisor and host-level audit logs for anomalous CMS message processing events or unexpected authentication failures originating from VM-to-hypervisor communication channels. Enable verbose logging on the cloud-hypervisor process if not already active (NIST AU-2: Event Logging; CIS 8.2: Collect Audit Logs). Look for unexpected process spawns or file modifications associated with the cloud-hypervisor binary. No published IOCs are present in the provided source data; behavioral indicators are the primary detection surface.
3. Step 3: Eradication. Apply the updated azl3 cloud-hypervisor package as distributed via the Microsoft June 2026 Patch Tuesday release. Use the Azure Linux package manager ('tdnf update cloud-hypervisor' on Azure Linux 3.0) and verify the installed version supersedes 51.1.56-1. Validate the update against the MSRC advisory (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-34182). If patching cannot be applied immediately, restrict CMS AuthEnvelopedData message paths at the hypervisor boundary where operationally feasible.
4. Step 4: Recovery. After patching, restart affected hypervisor processes and confirm the new package version is active. Re-run 'rpm -q cloud-hypervisor' to verify. Restore any workloads that were isolated during containment. Monitor hypervisor logs for 24-48 hours post-patch for residual anomalies (NIST AU-6: Audit Record Review, Analysis, and Reporting; NIST IR-5: Incident Monitoring). Validate workload isolation integrity for any VMs that shared hypervisor infrastructure during the exposure window.
5. Step 5: Post-Incident. Document the exposure window and affected hosts per NIST IR-8 (Incident Response Plan) requirements. Assess whether automated patch management cadences covered this package class (CIS 7.3: Perform Automated Operating System Patch Management; CIS 7.4: Perform Automated Application Patch Management). Review asset inventory completeness for cloud-hypervisor components (CIS 1.1: Establish and Maintain Detailed Enterprise Asset Inventory). Evaluate whether cryptographic integrity validation controls are audited as part of the standard vulnerability management process (CIS 7.1: Establish and Maintain a Vulnerability Management Process).

Detection Guidance

No published IOCs (hashes, IPs, domains) are present in the provided source data for CVE-2026-34182. Detection is behavioral and log-based. Query host-level audit logs on Azure Linux 3.0 nodes for unexpected authentication failures, errors, or warnings from the cloud-hypervisor process, particularly any events referencing CMS parsing or message authentication. Enable and collect audit logs per NIST AU-2 (Event

Logging) and AU-12 (Audit Record Generation); ensure logs are forwarded to a centralized SIEM (CIS 8.2: Collect Audit Logs). Monitor for anomalous inter-VM traffic patterns or unexpected VM-to-hypervisor IPC activity. Apply D3-SFA (System File Analysis) to monitor the cloud-hypervisor binary and its configuration files for unauthorized modification. Use D3-LAM (Local Account Monitoring) to detect any privilege escalation attempts on Azure Linux 3.0 hosts following successful exploitation. Confirm package version via 'rpm -q cloud-hypervisor' on all Azure Linux 3.0 nodes as a baseline check. Authoritative detection guidance beyond the above is not present in the provided source data; monitor MSRC and CISA for updated indicators.

Framework Mappings

MITRE-ATTACK

- **T1600** — Weaken Encryption
- **T1565** — Data Manipulation

CIS-V8

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

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information
- **A.8.24** — Use of cryptography
- **A.5.23** — Information security for use of cloud services

NIST-800-53R5

- **SC-13** — Cryptographic Protection

HIPAA-SECURITY

- **164.312(e)(1)** — Transmission Security

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1600	Weaken Encryption	Defense-Evasion
T1565	Data Manipulation	Impact

Sources

Source	URL	Tier
MSRC Update Guide	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-34182	T1

Source	URL	Tier
(consolidated)	https://api.msrc.microsoft.com/cvrf/v3.0/cvrf/2026-Jun	T1
CVE-2026-34182 - CVE Record	https://www.cve.org/CVERecord?id=CVE-2026-34182	T3
CVE-2026-34182 | Ubuntu	https://ubuntu.com/security/CVE-2026-34182	T3
CVE-2026-34182 Common Vulnerabilities and Exposures | SUSE	https://www.suse.com/security/cve/CVE-2026-34182.html	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-34182	T1

Generated 2026-06-15 06:40 UTC by TJS Security Command Center