NEXAVM TECHNOLOGIES AG

Hypervisor Vulnerability Management & Patching Policy

Infrastructure Security Assurance Technical White Paper

1. Executive Summary

As enterprise operations scale across private, hybrid, and distributed cloud computing architectures, the stability and structural security of the underlying virtualization layers become essential. NexaSphere is engineered following strict defense-in-depth principles, enforcing absolute isolation between infrastructure assets and customer workloads.

This policy framework provides formal documentation detailing NexaVM Technologies standardized lifecycle methodologies for proactive vulnerability detection, intelligence aggregation, and the automated escalation pipelines governing hotfix development and patch delivery. By adhering to these rigorous architectural standards, NexaVM guarantees data center resilience against zero-day threats, supply-chain risks, and targeted hypervisor exploits.

Strategic Security Standard: NexaSphere separates the management plane, control plane, and data plane. The hypervisor hosts run a highly minimized, locked-down Linux enterprise kernel, naturally eliminating up to 80% of common operating system attack vectors.

2. Vulnerability Detection and Threat Intelligence

To neutralize security vulnerabilities prior to their potential exploitation in production environments, NexaVM utilizes a dual-engine discovery network combining external real-time threat intelligence feeds with internal code security pipelines.

2.1 Real-Time Threat Intelligence Aggregation

NexaVM's dedicated Product Security Incident Response Team (PSIRT) continuously monitors global security channels, open-source communities, and enterprise Linux vendor security advisories. This comprehensive intelligence ingestion network tracks critical architectural subsystems including:

- **Enterprise KVM & QEMU Modules:** Monitoring for memory virtualization escapes, hardware emulation flaws, or malicious hypercalls.
- **Linux Kernel Components:** Ingesting updates from national vulnerability registries (including CVE, NVD, and CNNVD) relating to privilege escalation, network stack vulnerabilities, or driver defects.

- **Upstream Dependencies:** Tracking core system libraries, cryptographic modules (such as OpenSSL), and networking daemons integrated into the cloud ecosystem.

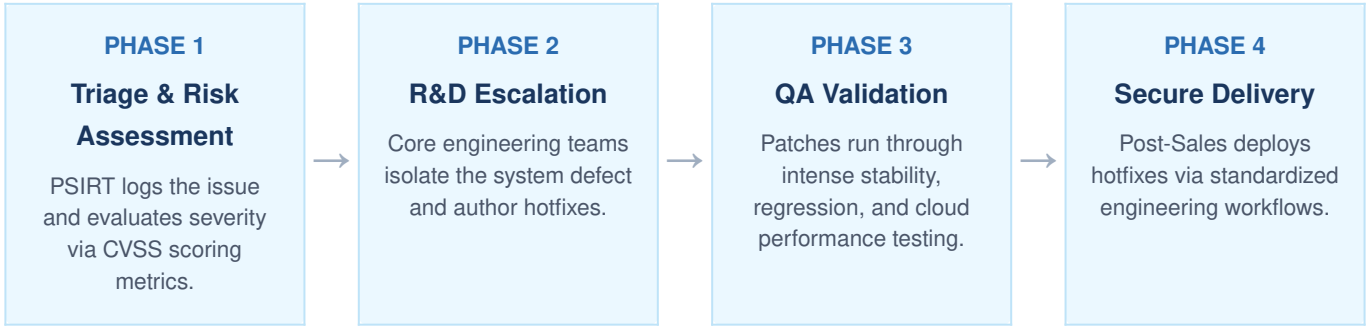
2.2 Internal Code Quality and Supply-Chain Security

Security is natively integrated directly into the NexaVM continuous integration and continuous deployment (CI/CD) pipelines:

- **Static Application Security Testing (SAST):** Automatic code scanning algorithms evaluate all internal product adjustments and feature updates to prevent logic flaws, injection capabilities, or authorization bypasses before compilation.
- **Software Bill of Materials (SBOM) Scanning:** Third-party components and binary dependencies undergo continuous composition analysis to eradicate legacy or inherited supply-chain vulnerabilities before software packaging.

3. Vulnerability Response and Patch Management Lifecycle

When an infrastructure or hypervisor-level vulnerability is confirmed, NexaVM activates an integrated response protocol designed to accelerate technical remediation while maintaining absolute enterprise business continuity.



3.1 Dedicated Research & Development Escalation

Upon vulnerability confirmation, the issue is immediately escalated to NexaVM's core R&D Engineering Division. This specialized unit isolates the underlying software defect and creates a target patch or alternative architectural configuration bypass. The escalation process is governed by strict Internal Service Level Agreements (SLAs) tailored to Common Vulnerability Scoring System (CVSS) benchmarks.

3.2 Advanced Mitigation and Cloud Workload Availability

Recognizing that enterprise data centers place an absolute priority on continuous runtime operations, NexaVM structures its patch delivery mechanism to maximize workload availability:

- **Virtual Machine Non-Disruption:** Patches, updates, and configuration mitigations are structured to protect and preserve running guest virtual machine environments, minimizing operational impact on active business layers.

- **High-Availability Architecture:** Leveraging cluster-level redundancies and migrations, security remediations can be seamlessly systematically integrated across the cloud fabric while maintaining active service endpoints.

3.3 Post-Sales Distribution and Enterprise Engineering Support

All certified system patches, hardened configuration binaries, and deployment advisories are formally released through NexaVM's technical post-sales support ecosystem. NexaVM's Enterprise Technical Support Engineers directly cooperate with the customer’s cloud infrastructure operations team to provide:

- Detailed pre-patch impact reports and structural environment evaluations.
- Step-by-step verification scripts to confirm correct patch installation.
- Guided implementation support during scheduled enterprise maintenance windows to assure successful system remediation.

Document Code: NVM-SEC-2026-V1 | **Classification:** Commercial in Confidence | **Published:** June 2026