CERT-IN VULNERABILITY NOTE: MULTIPLE VULNERABILITY IN NVIDIA ISAAC LAUNCHABLE

Vulnerability Note No.:	CIVN-2025-0388
Issue Date:	December 26, 2025
Severity Rating:	**CRITICAL**
Affected Platform:	NVIDIA ISAAC LAUNCHABLE

1. Overview

NVIDIA Isaac is a robotics development platform, and **Isaac Launchables** are **pre-built, ready-to-run workflows** that let developers quickly start, test, and deploy robotics applications without building everything from scratch.

They are designed to help teams **move faster from simulation to real robots** 🚀

2. What are Isaac Launchables?

Packaged robotics solutions	Built on **NVIDIA Isaac ROS**, **Isaac Sim**, and **Omniverse**	Optimized for **GPU-accelerated robotics**	Deployable on **real robots or simulation environments**

3. Description (As per CERT-In Vulnerability)

An **NVIDIA Isaac Launchable** is a preconfigured, cloud-based software environment for accessing NVIDIA Isaac Lab and Isaac Sim, designed to let developers start robotics projects without extensive local setup or configuration.

The "Launchable" is an installation and deployment option, typically provided in collaboration with a cloud service like NVIDIA Brev, which offers a streamlined, low-friction pathway for developers to access high-performance, preconfigured GPU resources.

4. Impact of Compromise (As per CERT-In)

1	Unauthorized access, RCE, privilege escalation, DoS
2	Robots could malfunction or be manipulated
3	Sensitive data/models can be stolen or tampered
4	Affects cloud, enterprise, industrial, and research systems

5. Recommendations for Individuals (As per CERT-In)

It is recommended to take following actions **user** planning to use **NVIDIA Isaac Launchables** (Isaac Sim, Isaac ROS, Isaac Lab, etc.), focusing on **cybersecurity, safe usage, and compliance best practices**.

✅ Individual Recommendations for NVIDIA Isaac Launchables (as per CERT-In best practices)

1. Secure System & Environment

- Use licensed OS and software only (Linux/Ubuntu recommended for Isaac).
- Keep OS, GPU drivers, CUDA, Isaac SDKs fully updated.
- Enable automatic security updates wherever possible.

2. Download from Trusted Sources Only

- Download Isaac Launchables **only from NVIDIA official sources** (NVIDIA Developer Portal, GitHub verified repos).
- Avoid cracked, modified, or third-party distributions.

3. Account & Credential Security

- Use **strong, unique passwords** for:
  - NVIDIA Developer account
  - GitHub / Docker Hub accounts
- Enable **Multi-Factor Authentication (MFA)** on all developer accounts.
- Never share **API keys, tokens, or credentials** in public repos.

4. Secure Docker & Containers (Very Important for Isaac)

- Pull Docker images **only from official NVIDIA registries**.
- Regularly scan containers for vulnerabilities.
- Do **not run containers as root** unless required.
- Close unused ports and services.

6. Recommendations for Organizations (As per CERT-In)

Organizations intending to deploy **NVIDIA Isaac Launchables** for robotics, AI simulation, and autonomous systems should ensure alignment with **CERT-In cybersecurity best practices and statutory requirements** to maintain a secure, resilient, and compliant technology environment.

1. Governance & Compliance

- Ensure compliance with **CERT-In Directions (2022)** related to:
  - Cyber incident reporting within **6 hours**
  - Log retention for a minimum of **180 days**
- Define clear **ownership and accountability** for AI/robotics platforms within the organization.
- Establish an **AI & Robotics Security Policy** aligned with ISO/IEC 27001 and CERT-In advisories.

2. Secure Infrastructure Deployment

- Deploy Isaac Launchables only on **hardened systems** (secure OS images, patched kernels, minimal services).
- Use **secure containers and virtualization** with role-based access control (RBAC).
- Isolate simulation, training, and production environments to reduce lateral movement risks.

3. Access Control & Identity Management

- Enforce **strong authentication** (MFA) for access to NVIDIA Omniverse, Isaac Sim, and related services.
- Apply **least privilege principles** for developers, operators, and third-party vendors.
- Maintain audit trails for all access to AI models, simulation data, and robotics control systems.

4. Data Protection & Privacy

- Classify data used in simulations and training (sensor data, maps, logs).
- Encrypt data:
- At rest (disk-level or database encryption)
- In transit (TLS 1.2+)

- Ensure sensitive or proprietary data is not exposed in shared or cloud-based simulation environments.

5. Vulnerability & Patch Management

- Regularly monitor CERT-In advisories, NVIDIA security bulletins, and CVE disclosures.
- Apply timely **patches and updates** to:
  - NVIDIA drivers
  - CUDA, Omniverse, and Isaac SDK components
- Conduct **periodic vulnerability**

6. Logging, Monitoring & Incident Response

- Enable centralized logging for:
  - System events
  - AI workloads
  - Network traffic
- Integrate logs with a **SIEM/SOC** for real-time monitoring.
- Update the **Cyber Security Incident Response Plan (CSIRP)** to include AI/robotics-specific incidents.
- Report significant incidents to CERT-In within the mandated timeframe.

7. Third-Party & Supply Chain Risk

- Evaluate security posture of vendors, cloud providers, and system integrators supporting Isaac Launchables.
- Use only **verified and trusted NVIDIA repositories** and container images.
- Maintain SBOM (Software Bill of Materials) for AI and robotics components where feasible.

Best Practices as per CERT-In Guidelines:

Secure Development & Deployment

- **Least Privilege:** Run services and processes with the minimum necessary permissions.
- **Secure Credential Management:** Avoid hard-coding secrets in code or configurations — use secret managers (e.g., Vault, KMS).
- **Configuration Hardening:** Disable unused services and secure default settings by design.

✔ Patch Management

Establish a formal patching process with timelines based on severity.

- Prioritize fixes for critical vulnerabilities and test patches in staging before production.

✔ Logging & Monitoring

- Enable audit logging for access and execution events.
- Use SIEM or monitoring tools to detect suspicious behaviors.

✔ Risk Assessment

- Perform periodic security assessments and review configurations against standards such as OWASP, ISO/IEC 27001, and CIS benchmarks. CDN BBSR

Network and Access Controls

- Restrict Access: Limit network exposure of Isaac Launchable components using firewalls and VPNs.
- Microsegmentation: Isolate critical robotics environments into dedicated network segments.
- Zero Trust: Authenticate and authorize every connection, even within trusted networks.

Pre-deployment Validation

- Test new releases for configuration and security issues before rolling them out broadly.
- Use automated tools to scan for known vulnerabilities at build time.

Runtime Protection

- Limit execution rights and disable privileged modes unless absolutely needed.
- Apply application whitelisting and container/runtime security policies where possible.

Monitoring & Incident Readiness

- Implement real-time intrusion detection or anomaly detection tools.
- Define and test an incident response plan tailored to robotics/automation stacks.

Build a Security Culture Around AI/Robotics Systems

- Because Isaac Launchable often runs in environments involving physical robots or critical automation:
- Train teams on secure coding and deployment practices.
- Review third-party dependencies, ensuring they follow secure development practices.
- Conduct periodic threat modeling and risk assessments specifically for robotics/AI pipelines.

References

Vulnerability	Details
CERT-In Website	https://www.cert-in.org.in/

CVE NAME

CVE-2025-33222
CVE-2025-33223
CVE-2025-33224

KNOWLEDGE DESK

CISA Altamash Shaikh

CISA Shraddha Godbole

CISA Taher Pepermintwala
Alefiya Songirwala