CASTELLUM LABS

WEEKLY DIGEST

VULNERABILITIES

Reporting Period – 21 JUNE – 27 JUNE 2026

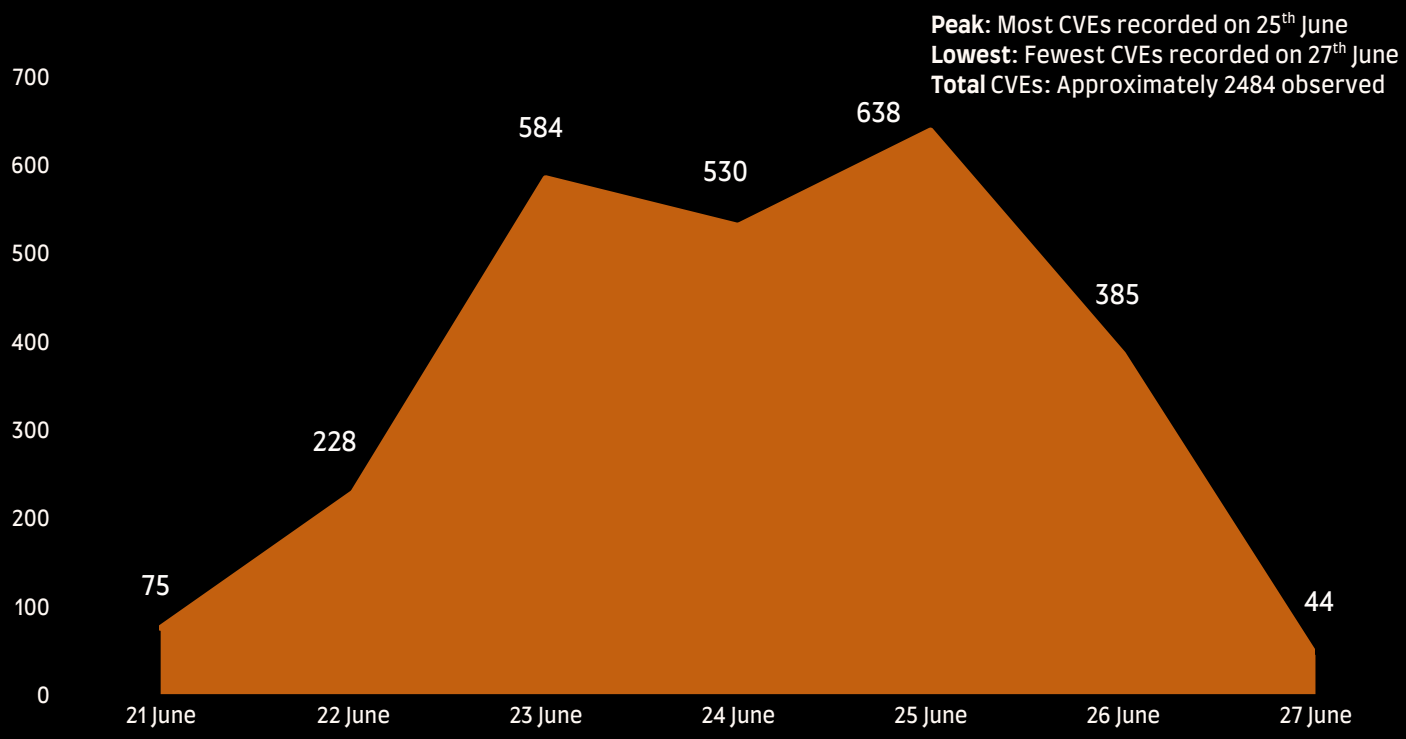
enisa EUROPEAN UNION VULNERABILITY DATABASE

NIST CVE

OSV

CISA America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Number of CVE this week



Top CVE this week

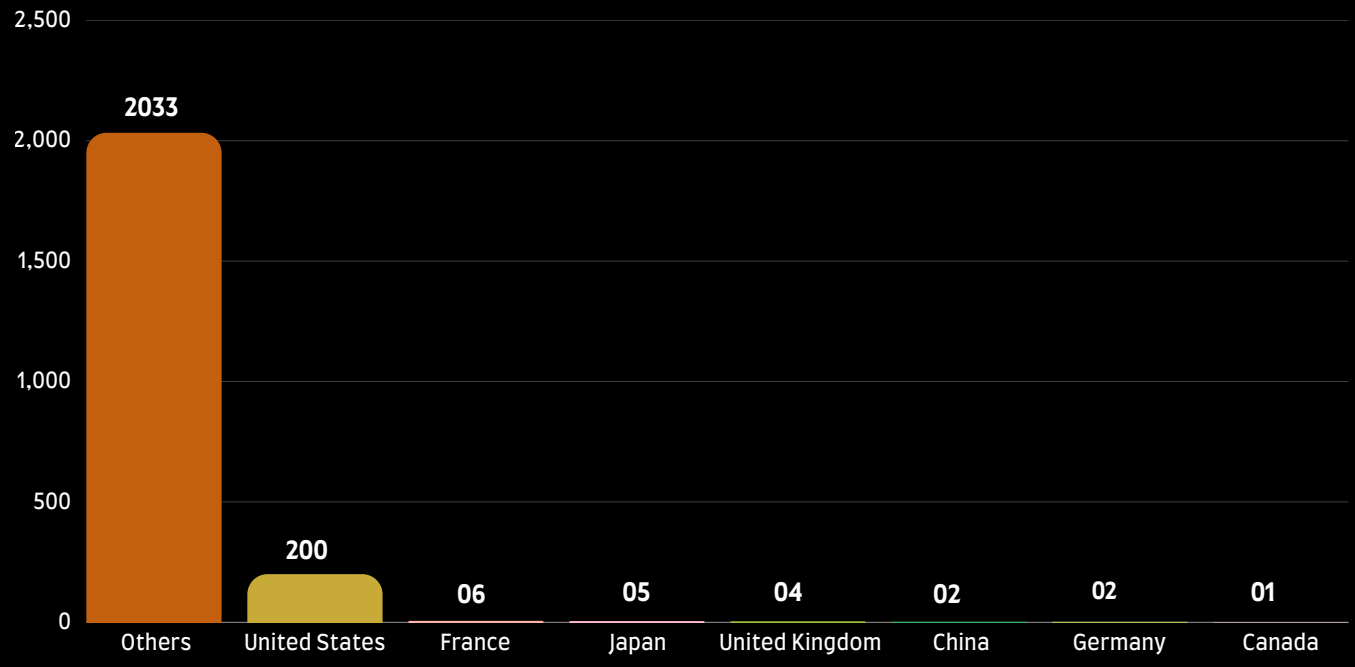
CVE ID	CVSS Score	Severity
CVE-2026-10561	10.0	Critical
CVE-2026-12485	10.0	Critical
CVE-2025-71338	10.0	Critical
CVE-2026-54350	10.0	Critical
CVE-2025-70974	10.0	Critical
CVE-2026-53576	10.0	Critical

KEY HIGHLIGHTS

This week's top five vulnerabilities reveal critical software and network weaknesses, with some already actively exploited, requiring urgent remediation.

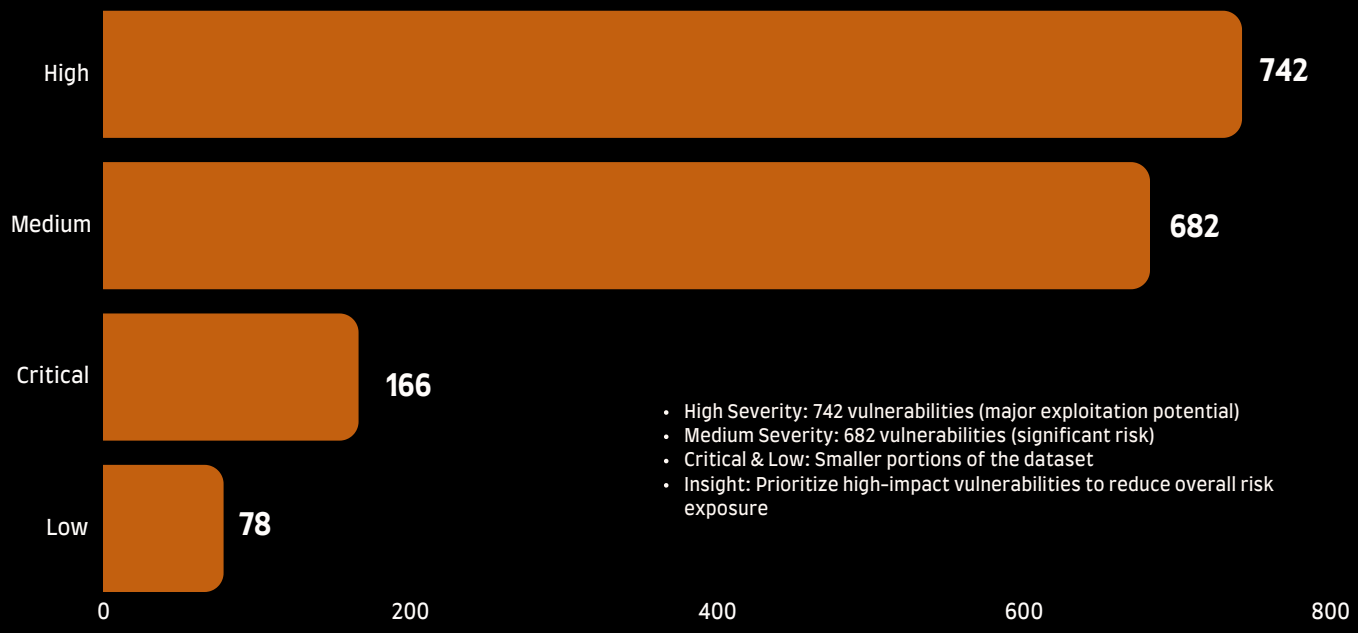
+91 7842046995 reach@castellumlabs.com www.castellumlabbs.com

Top Affected Vendors



Analysis of CVE-affected vendors reveals that a majority fall under the “Others” category, suggesting a highly distributed global impact across multiple countries.

Severity Breakdown



- High Severity: 742 vulnerabilities (major exploitation potential)
- Medium Severity: 682 vulnerabilities (significant risk)
- Critical & Low: Smaller portions of the dataset
- Insight: Prioritize high-impact vulnerabilities to reduce overall risk exposure

Most CVEs (93.3%) have fixes available, but 6.7% remain unpatched, emphasizing the ongoing risk and the importance of timely patching.

+91 7842046995 reach@castellumlabs.com www.castellumlabbs.com

CVE-2026-10561

Overview

A critical vulnerability has been identified in IBM Langflow OSS that allows unauthenticated remote code execution through improper isolation of Python execution and an authentication bypass. A remote attacker can exploit the flaw to execute arbitrary code on the host system, potentially resulting in complete system compromise.

Technical Details

The vulnerability is caused by improper isolation of the PythonREPLComponent combined with an authentication bypass. An unauthenticated attacker can inject malicious code into the Python execution environment through builtins manipulation, allowing arbitrary code execution on the underlying host. Successful exploitation can lead to full compromise of the affected system.

Vendor: **IBM**
Affected Product: **IBM Langflow OSS**
Affected Versions: **1.0.0 through 1.9.3**

- **Published Date:** 22-06-2026
- **Last Patch:** 22-06-2026
- **Vulnerability Type:** Improper Control of Generation of Code (CWE-94)
- **Fix Available:** Yes
- **Patched Version:** Later than 1.9.3 (upgrade to the latest available fixed release)

Exploitaion Status

- Exploite Status : No Known Exploitation
- Threat Actors / Malware: None reported
- Exploit Availability: Public Technical Advisory Available

Reference: https://www.ibm.com/support/pages/node/7277242

+91 7842046995 reach@castellumlabs.com www.castellumlabbs.com

CVE-2026-12485

Overview

A critical stack-based buffer overflow vulnerability has been identified in GeoVision GV-I/O Box 4E that could allow a remote attacker to execute arbitrary code. The flaw exists in the DVRSearch service, which listens for unauthenticated UDP requests, enabling attackers on the network to trigger memory corruption and potentially gain control of the affected device.

Technical Details

The vulnerability resides in the DVRSearch service, which runs by default and listens on UDP port 10001. Due to improper bounds checking during processing of the CMD_IP_SET command, attacker-controlled input can trigger a stack-based buffer overflow when the service copies the configured IP address into a reply buffer using an unsafe memory operation. Successful exploitation may allow arbitrary code execution or complete compromise of the device.

Vendor: **GeoVision Inc.**
Affected Product: **GeoVision GV-I/O Box 4E**
Affected Versions: **V2.09**

- **Published Date:** 24-06-2026
- **Last Patch:** 24-06-2026
- **Vulnerability Type:** Stack-based Buffer Overflow (CWE-121)
- **Fix Available:** Yes
- **Patched Version:** v2.12

Exploitation Status

- Exploited in the Wild: No known exploitation
- Threat Actors / Malware: None reported
- Exploit Availability: Public technical advisory available

Reference: https://www.geovision.com.tw/cyber_security.php

+91 7842046995 reach@castellumlabs.com www.castellumlabbs.com

CVE-2025-71338

Overview

A critical vulnerability has been identified in Flowise that allows unauthenticated attackers to write arbitrary files to the underlying filesystem through a path traversal flaw. By exploiting the vulnerable document-store API endpoint, an attacker can overwrite critical application files and achieve remote code execution after the application restarts.

Technical Details

The vulnerability exists in the /api/v1/document-store/loader/process endpoint due to insufficient validation of the fileName parameter. An attacker can supply directory traversal sequences (../) to write arbitrary files outside the intended directory. By overwriting critical application files, such as package.json, an attacker can execute arbitrary code when the Flowise application is restarted, resulting in complete system compromise.

Affected Product: **Flowise**
Affected Versions: **Not Available**
Vendor: **Flowise**

- **Published Date:** 25-06-2026
- **Last Patch:** 25-06-2026
- **Vulnerability Type:** External Control of File Name or Path (CWE-73)
- **Fix Available:** Yes
- **Patched Version:** Not Available

Exploitation Status

- Exploited in the Wild: No known exploitation
- Threat Actors / Malware: None reported
- Exploit Availability: Public vendor advisory available

Reference: https://github.com/FlowiseAI/Flowise/security/advisories/GHSA-8vvx-qvq9-5948

+91 7842046995 reach@castellumlabs.com www.castellumlabbs.com

CVE-2026-54350

Overview

A critical vulnerability has been identified in Budibase that allows unauthenticated attackers to perform NoSQL operator injection through published application query templates. By exploiting improper input validation, an attacker can read all documents from backend data sources and, where public write queries are enabled, modify all documents with a single request.

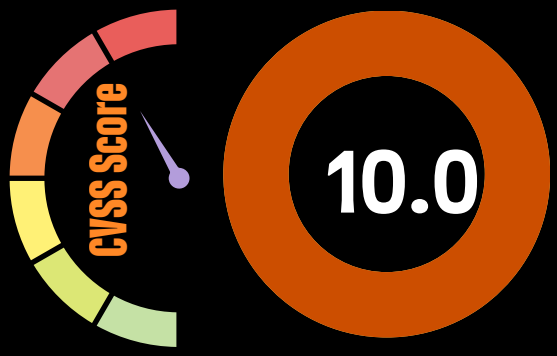
Technical Details

The vulnerability exists because user-supplied parameters are inserted into raw JSON query bodies without properly escaping JSON metacharacters before parsing. An attacker can inject NoSQL operators into query parameters, altering the intended query logic.

Budibase

Affected Product: **Budibase**
Affected Versions: **Prior to 3.39.12**
Vendor: **Budibase**

- **Published Date:** 26-06-2026
- **Last Patch:** 26-06-2026
- **Vulnerability Type:** Improper Neutralization of Special Elements in Data Query Logic (CWE-943)
- **Fix Available:** Yes
- **Patched Version:** 3.39.12



Exploitation Status

- Exploited in the Wild: No known exploitation
- Threat Actors / Malware: None reported
- Exploit Availability: Public technical advisory available

Reference: https://github.com/Budibase/budibase/security/advisories/GHSA-8qv3-p479-cj62

+91 7842046995 reach@castellumlabs.com www.castellumlabbs.com

CVE-2025-70974

Overview

A critical vulnerability has been identified in Alibaba Fastjson that allows remote code execution through insecure handling of the autoType feature. An attacker can supply a malicious Java class reference within a JSON payload, potentially triggering JNDI injection and arbitrary code execution. The vulnerability has been actively exploited in the wild.

Technical Details

The vulnerability exists because Fastjson improperly handles the autoType feature when processing JSON documents containing an @type field. An attacker can specify the name of a Java class that causes Fastjson to invoke public methods during deserialization. Depending on the behavior of the targeted class, this can lead to JNDI injection using attacker-controlled data within the JSON payload, ultimately resulting in remote code execution. This issue is due to an incomplete fix for CVE-2017-18349, while a separate bypass is addressed by CVE-2022-25845.

Affected Product: **Alibaba Fastjson**
Affected Versions: **Before 1.2.48**
Vendor: **Alibaba**

- **Published Date:** 09-01-2026
- **Last Patch:** 27-06-2026
- **Vulnerability Type:** Remote Code Execution (RCE)
- **Fix Available:** Yes
- **Patched Version:** 1.2.48

Exploitation Status

- Exploited in the Wild: Exploited in the Wild
- Threat Actors / Malware: None reported
- Exploit Availability: Public exploit code and technical research available

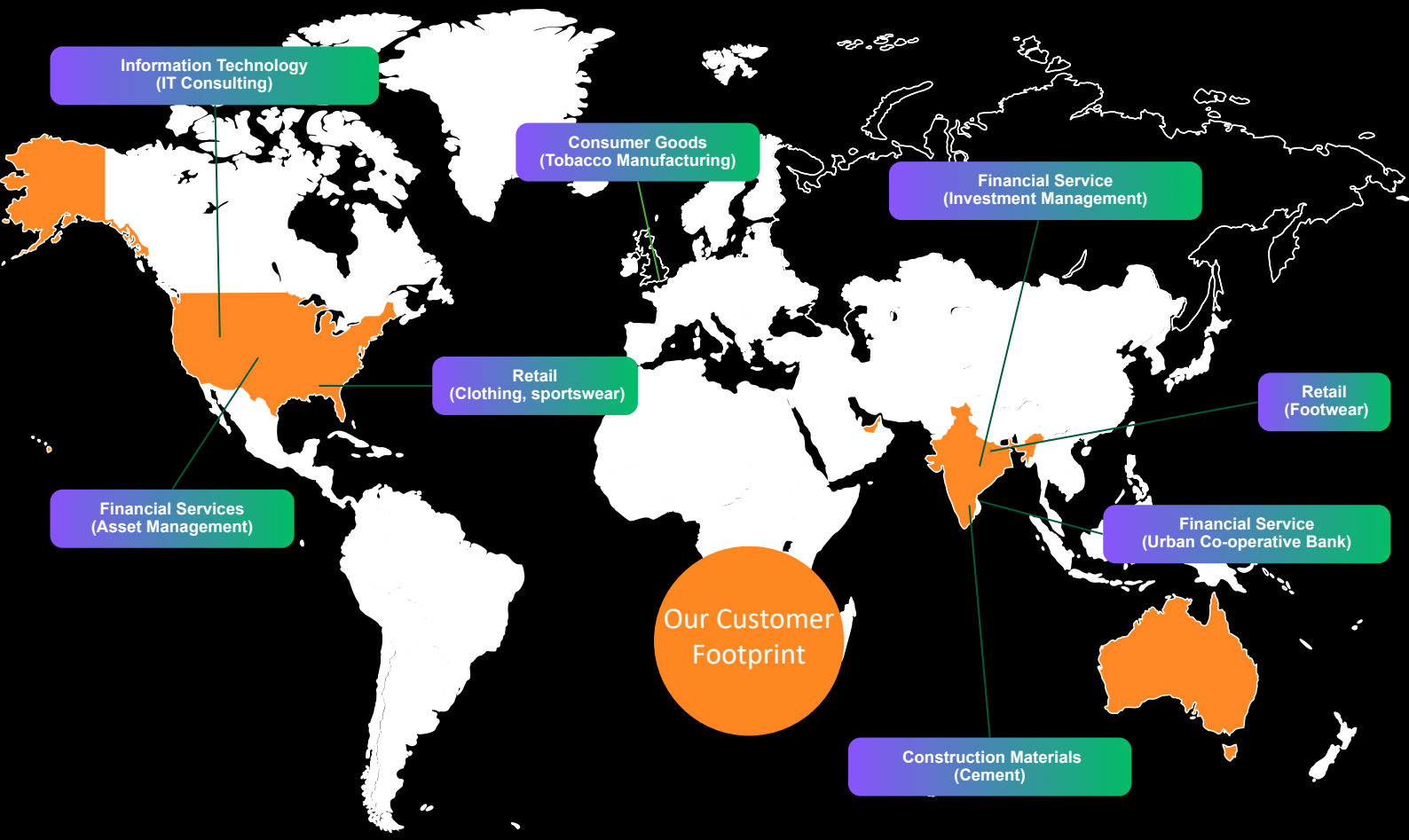
Reference: https://www.seebug.org/vuldb/ssvid-98020

+91 7842046995 reach@castellumlabs.com www.castellumlabbs.com

About Castellum Labs

- Services delivered by Global Cyber Capability Center using advance Platforms
- Based in Hyderabad, India with global customer base across India, US, Europe
- Strong Handpicked Team of 50+ with (best of security talent globally)
- Started by people with decades of product, services & deep tech experience
- Subscription & annual contract modeled services delivered globally
- Value + Impact from Day One, No Installation & No Deployment

100's of Satisfied Customers Across the Globe!



Cyber Security Portfolio

Secure Cloud WL

- Design Security for Cloud
- Cloud Security Posture
- DevOps Infra Security
- Container Security
- Kubernetes Security
- Integrated S/W Security
- Workload Hardening
- Security Automation
- Cloud Native Monitoring
- Cloud Governance

We create secure cloud environments, automate Cloud SecOps & manage it.

24x7 Monitoring

- MDR, 24x7 Monitoring
- SOC as a Service
- SIEM/SOC Design & Impl
- SOC Team on Hire
- Managed Incidents
- IR Process Designs
- IR Workshops
- SOC Assessments
- Threat Hunting Services
- Forensic Services

When it comes to SOC Monitoring & Response, we cover all aspects of it

Vuln Mgmt

- Application Security
- Network VAPT
- Cloud VAPT
- Controls & Config Audit
- Program Design for VAPT
- Managed Vuin Programs
- VAPT Automations
- Surface Assessments
- Threat Intel for VAPT
- DevSecOps

Program designed VAPT Engagement to enhance protection & reduce attack surface

Threat Intel

- Threat Intel Solutions
- Darkweb Hunting
- Deep Intel Reports
- Threat Intel Integrations
- Intelligence Automations
- Threat Intel Curation
- Vectored Searches
- Data Hunting
- Threat Intel Architecture
- Adversary Tracking

We take threat intel maintenance, keep, usage & application to next level.

Data & Privacy

- Data Security Design
- Data Sec Posture Assmnt
- Data Sec Posture Mgmt
- Encryption Design & Sol
- Data Exfiltration Assmnt
- Privacy Designing
- Privacy Gap Assessment
- Privacy Adoption Service
- Privacy Automations
- Privacy Compliances

Data and privacy are two considerations, we design, implement it & run compliances

Unified View of Security ...

#1 Orchestration & Automation

Automated governance
SecOps automation
Automated response

#2 Attack Surface Reduction

Inline AS detection
External AS validation
Continuous remediation

#3 Real Time Detection & Response

Real time detection
Active threat hunting
Proactive responses

#4 Zero Trust Micro Architecture

Zoning and isolations
Contextual runtime set
Transient access model

Castellum Labs

www.castellumlabs.com

Castellum Labs

reach@castellumlabs.com

+91 7842046995