CASTELLUM LABS

WEEKLY DIGEST

VULNERABILITIES

Reporting Period – 28 JUNE – 04 JULY 2026

enisa EUROPEAN UNION VULNERABILITY DATABASE

NIST CVE

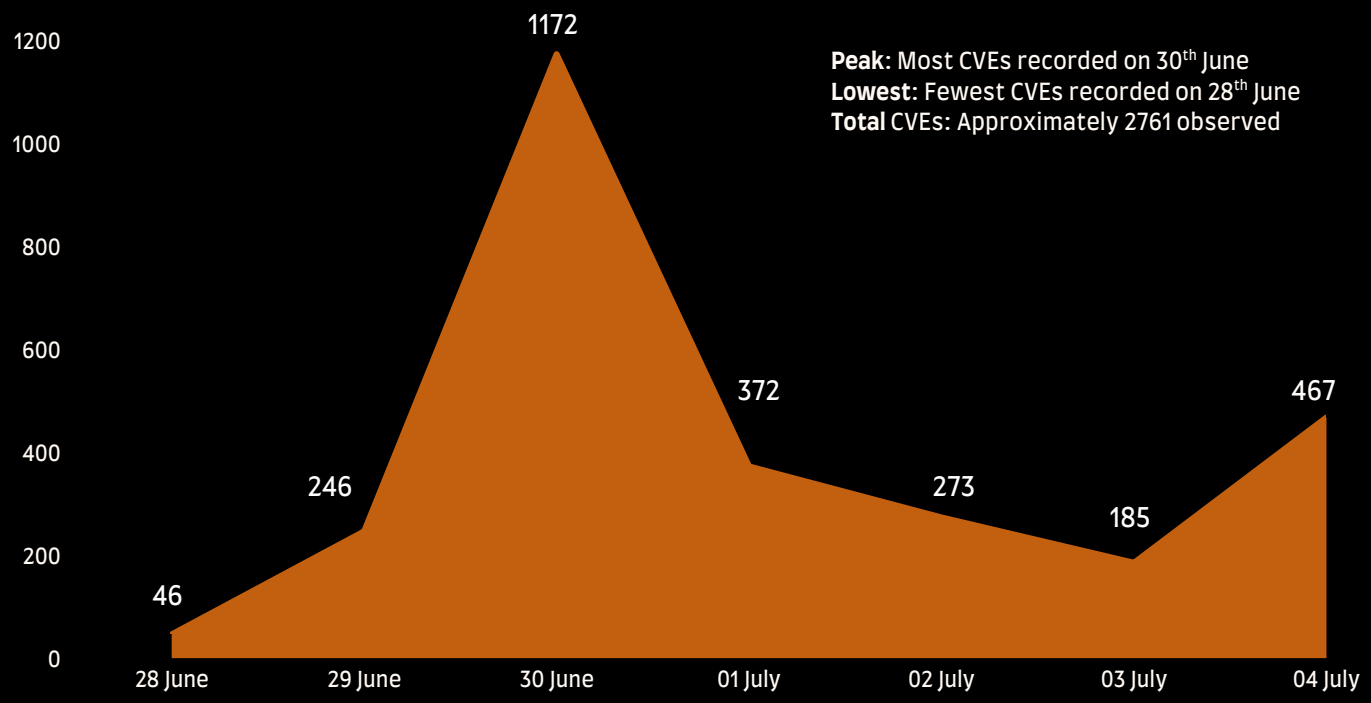
OSV

CISA CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Number of CVE this week



Top CVE this week

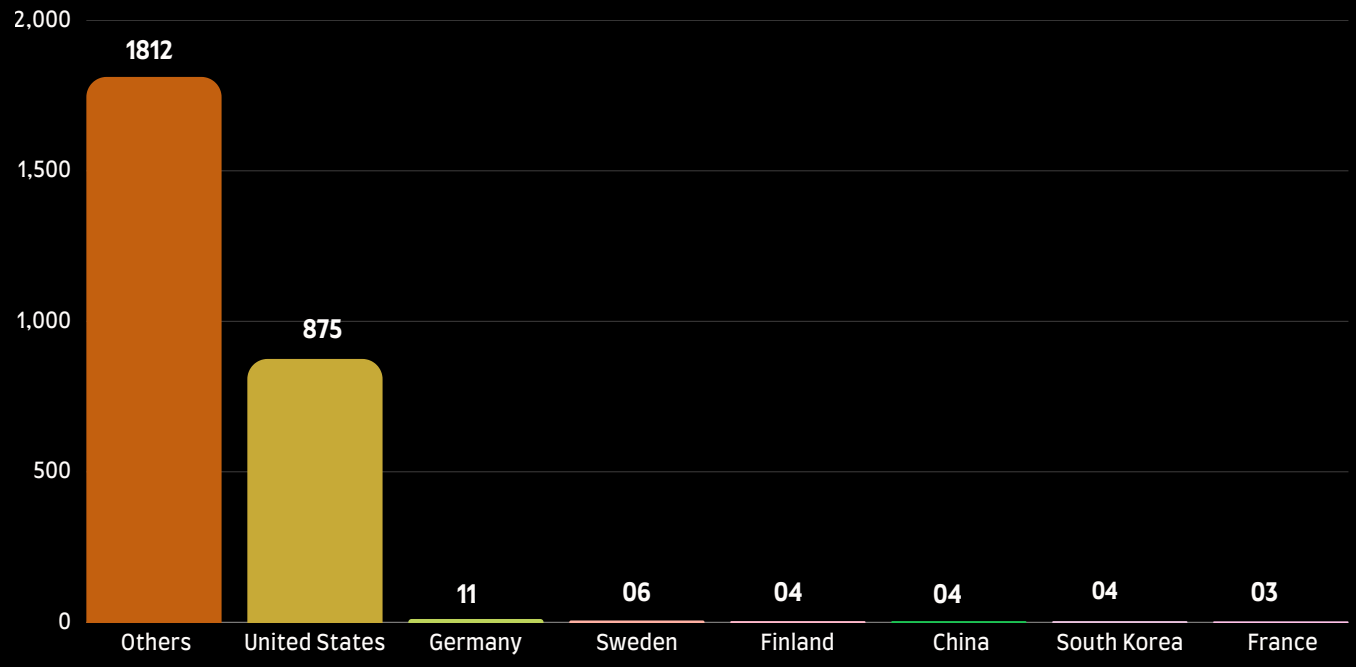
CVE ID	CVSS Score	Severity
CVE-2025-15379	10.0	Critical
CVE-2026-48286	10.0	Critical
CVE-2026-56415	10.0	Critical
CVE-2026-50746	10.0	Critical
CVE-2026-56004	10.0	Critical
CVE-2026-13768	10.0	Critical

KEY HIGHLIGHTS

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

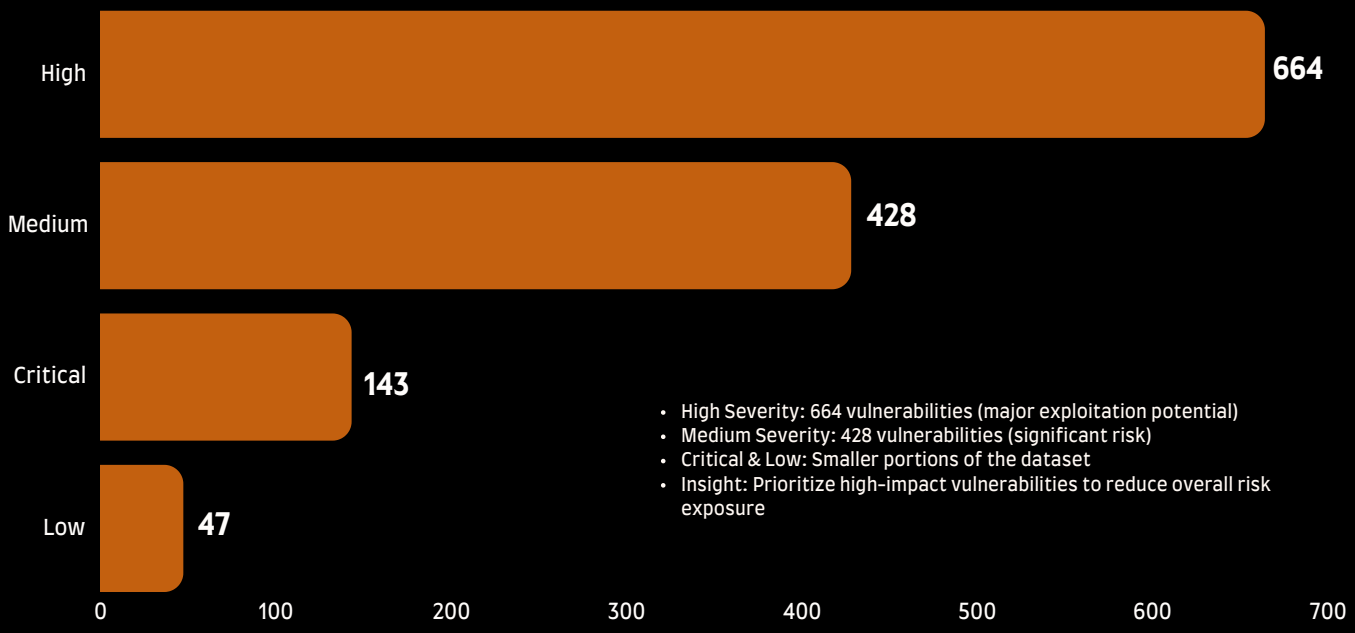
+91 7842046995 reach@castellumlabs.com www.castellumlabbs.com

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: 664 vulnerabilities (major exploitation potential)
- Medium Severity: 428 vulnerabilities (significant risk)
- Critical & Low: Smaller portions of the dataset
- Insight: Prioritize high-impact vulnerabilities to reduce overall risk exposure

Most CVEs (74.4%) have fixes available, but 25.6% remain unpatched, emphasizing the ongoing risk and the importance of timely patching.

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

CVE-2025-15379

Overview

A critical vulnerability has been identified in MLflow that allows command injection during model deployment. An attacker can craft a malicious model artifact containing a manipulated python_env.yaml file, which may result in arbitrary operating system command execution when the model is deployed using env_manager=LOCAL.

Technical Details

The vulnerability exists in MLflow's _install_model_dependencies_to_env() function, which processes dependency specifications from the model artifact's python_env.yaml file. The dependency values are directly incorporated into a shell command without proper input sanitization. By supplying a malicious model artifact with crafted dependency entries, an attacker can inject arbitrary commands that execute on the host system during model deployment when env_manager=LOCAL is used.

Vendor: **MLflow**
Affected Product: **MLflow (mlflow/mlflow)**
Affected Versions: **Before 3.8.2 (including 3.8.0)**

- **Published Date:** 30-03-2026
- **Last Patch:** 30-03-2026
- **Vulnerability Type:** Command Injection (CWE-77)
- **Fix Available:** Yes
- **Patched Version:** 3.8.2

Exploitaion Status

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

Reference: https://huntr.com/bounties/dc9c1c20-7879-4050-87df-4d095fe5ca75

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

CVE-2026-48286

Overview

A critical vulnerability has been identified in Adobe Campaign Classic (ACC) that allows arbitrary code execution due to an incorrect authorization flaw. An unauthenticated attacker can exploit this vulnerability over the network without requiring user interaction, potentially executing arbitrary code in the context of the current user.

Technical Details

The vulnerability is caused by an Incorrect Authorization (CWE-863) flaw in Adobe Campaign Classic. Improper authorization checks allow an unauthenticated remote attacker to perform unauthorized actions that can lead to arbitrary code execution in the context of the current user. Exploitation does not require user interaction and may impact additional components due to a scope change.

Vendor: **Adobe**
Affected Product: **Adobe Campaign Classic (ACC)**
Affected Versions: **7.4.3 build 9396 and earlier**

- **Published Date:** 30-06-2026
- **Last Patch:** 30-06-2026
- **Vulnerability Type:** Incorrect Authorization (CWE-863)
- **Fix Available:** Yes
- **Patched Version:** Later than Adobe Campaign Classic 7.4.3 build 9396

Exploitation Status

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

Reference: https://helpx.adobe.com/security/products/campaign/apsb26-69.html vendor-advisory

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

CVE-2026-56415

Overview

A critical vulnerability has been identified in StoneFly Storage Concentrator that allows unauthenticated remote command execution. An attacker can send a specially crafted HTTP request to a vulnerable debug script, resulting in arbitrary operating system command execution with root-level privileges on the underlying system.

Technical Details

The vulnerability exists in the debug.pl script of StoneFly Storage Concentrator, which is accessible without authentication. The script fails to properly sanitize user-supplied input before passing it to the operating system, allowing a remote attacker to inject arbitrary OS commands through a specially crafted HTTP request. Successful exploitation results in arbitrary command execution with root-level privileges, leading to complete system compromise.

Affected Product: **StoneFly Storage Concentrator (SC & SCVM)**
Affected Versions: **Before 8.0.4.22**
Vendor: **StoneFly**

- **Published Date:** 30-06-2026
- **Last Patch:** 30-06-2026
- **Vulnerability Type :** OS Command Injection (CWE-78)
- **Fix Available:** Yes
- **Patched Version:** 8.0.4.29

Exploitation Status

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

Reference:
https://github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2026/icsa-26-181-06.json

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

CVE-2026-50746

Overview

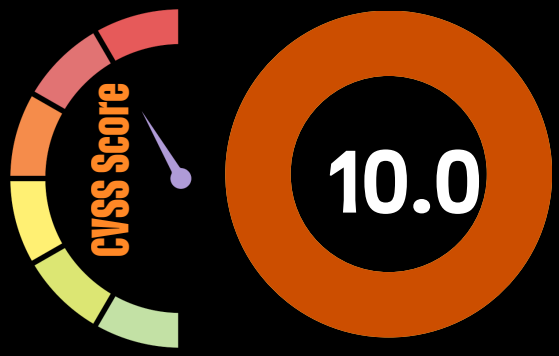
A critical vulnerability has been identified in the UniFi Connect Application that allows command injection due to an improper access control flaw. A remote attacker with network access can exploit the vulnerability to execute arbitrary operating system commands on the host device, potentially leading to complete system compromise.

Technical Details

The vulnerability is caused by Improper Access Control (CWE-284) within the UniFi Connect Application. Insufficient access restrictions allow a malicious actor with network access to reach functionality that can be abused to perform command injection on the underlying host device. Successful exploitation enables arbitrary operating system command execution, compromising the confidentiality, integrity, and availability of the affected system.

Affected Product: **UniFi Connect Application**
Affected Versions: **Before 3.4.20**
Vendor: **Ubiquiti Inc.**

- **Published Date:** 02-07-2026
- **Last Patch:** 02-07-2026
- **Vulnerability Type:** Improper Access Control (CWE-284)
- **Fix Available:** Yes
- **Patched Version:** 3.4.20



Exploitation Status

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

Reference: https://community.ui.com/releases/Security-Advisory-Bulletin-066-066/984eceb3-49c8-4227-942d-671c289b3afc

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

CVE-2026-56004

Overview

A critical vulnerability has been identified in openSUSE Build Service (obs-service-tar_scm) that allows command injection through its Mercurial handler. An attacker who can supply a malicious _service file can execute arbitrary commands as the source service or the local user processing the malicious service configuration.

Technical Details

The vulnerability exists in the Mercurial handler of the obs-service-tar_scm source service due to improper neutralization of special characters before constructing shell commands. An attacker able to provide a crafted _service file can inject arbitrary shell commands, resulting in code execution with the privileges of the source service or the local user checking out the malicious service.

Affected Product: **openSUSE Build Service**
Affected Versions: **Before 0.12.4**
Vendor: **openSUSE**

- **Published Date:** 02-07-2026
- **Last Patch:** 02-07-2026
- **Vulnerability Type:** OS Command Injection (CWE-78)
- **Fix Available:** Yes
- **Patched Version:** 0.12.4

Exploitation Status

- Exploited in the Wild: No Known Exploited
- Threat Actors / Malware: None reported
- Exploit Availability: Technical advisories available

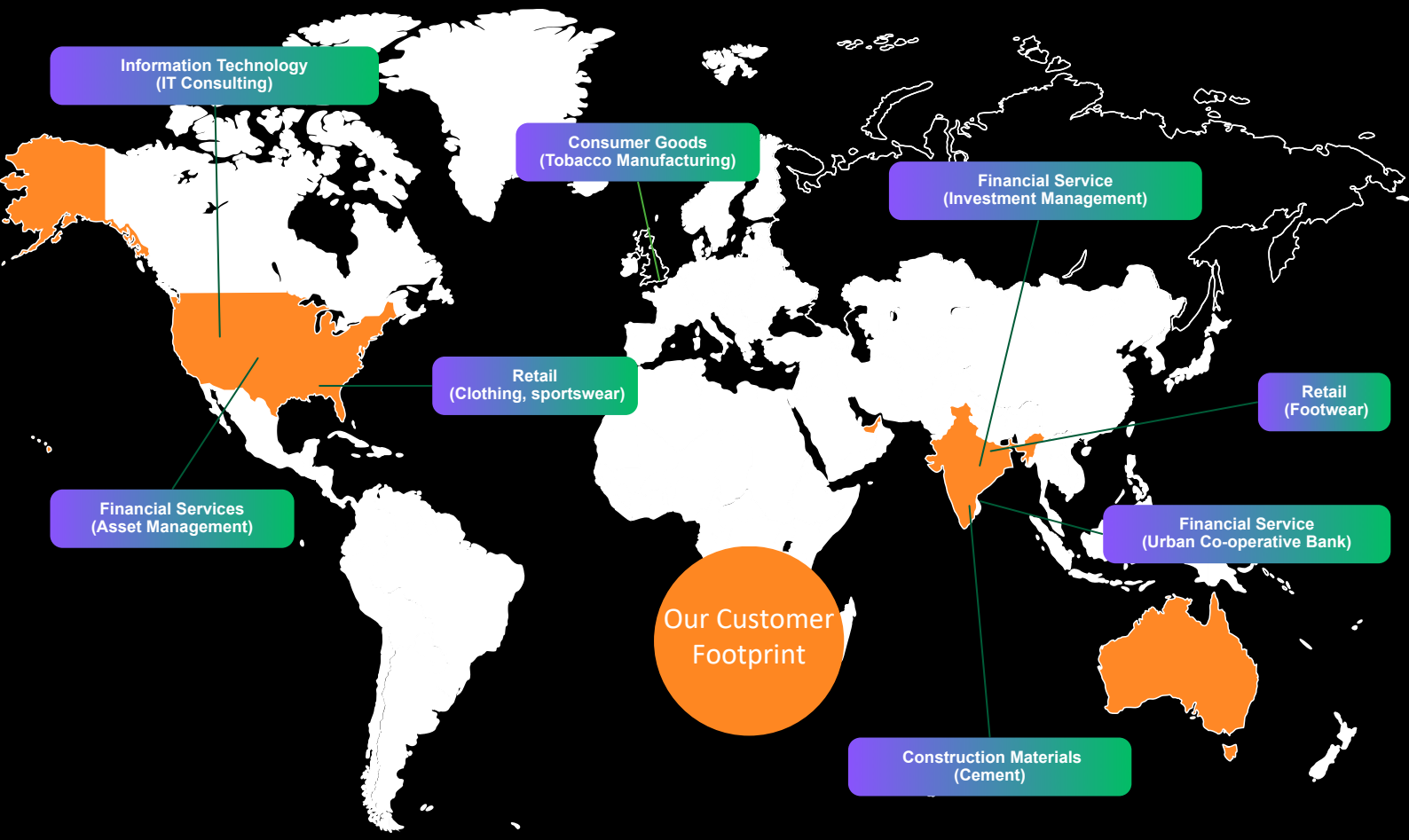
Reference:
https://github.com/openSUSE/obs-service-tar_scm/pull/552/changes/bcf29d318c671c45fe87dd9f995a4a0c78ecedd7

+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