CASTELLUM LABS

WEEKLY DIGEST

VULNERABILITIES

Reporting Period – 31 MAY – 06 JUNE 2026

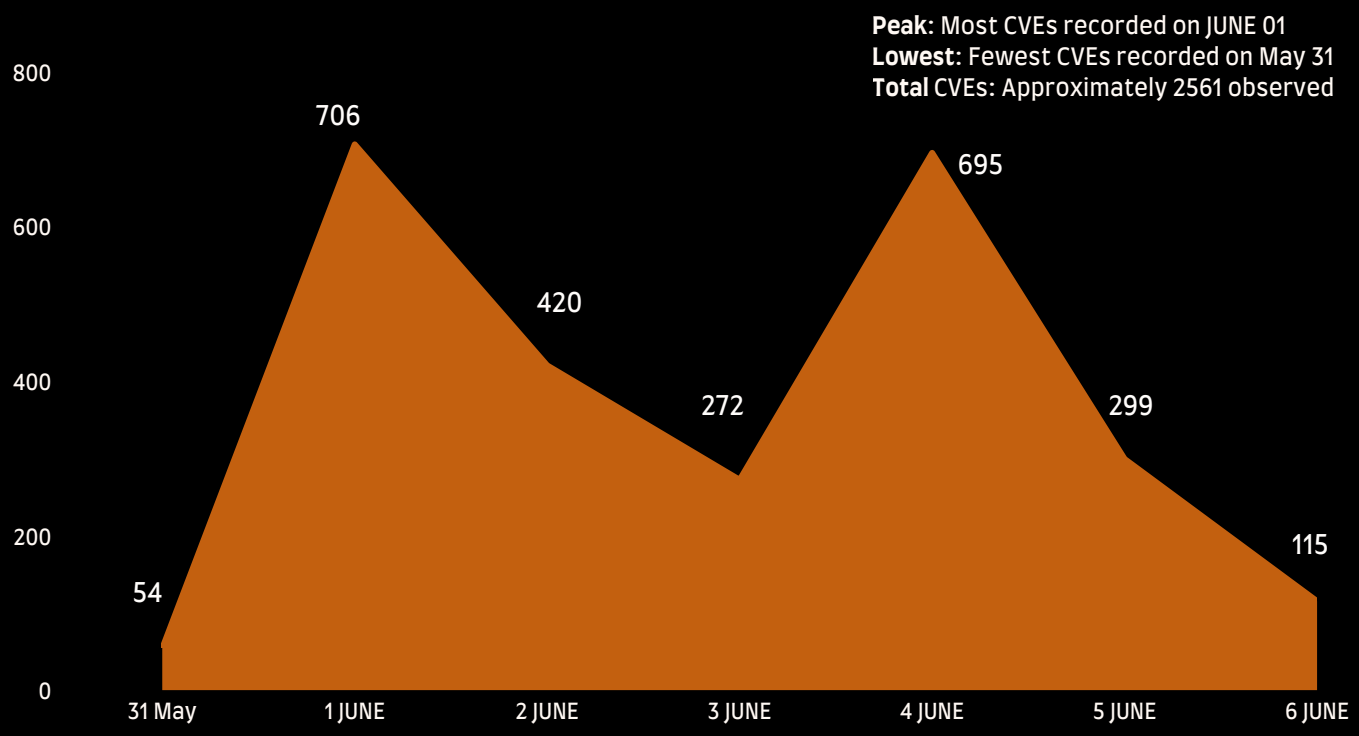
enisa EUROPEAN UNION VULNERABILITY DATABASE

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

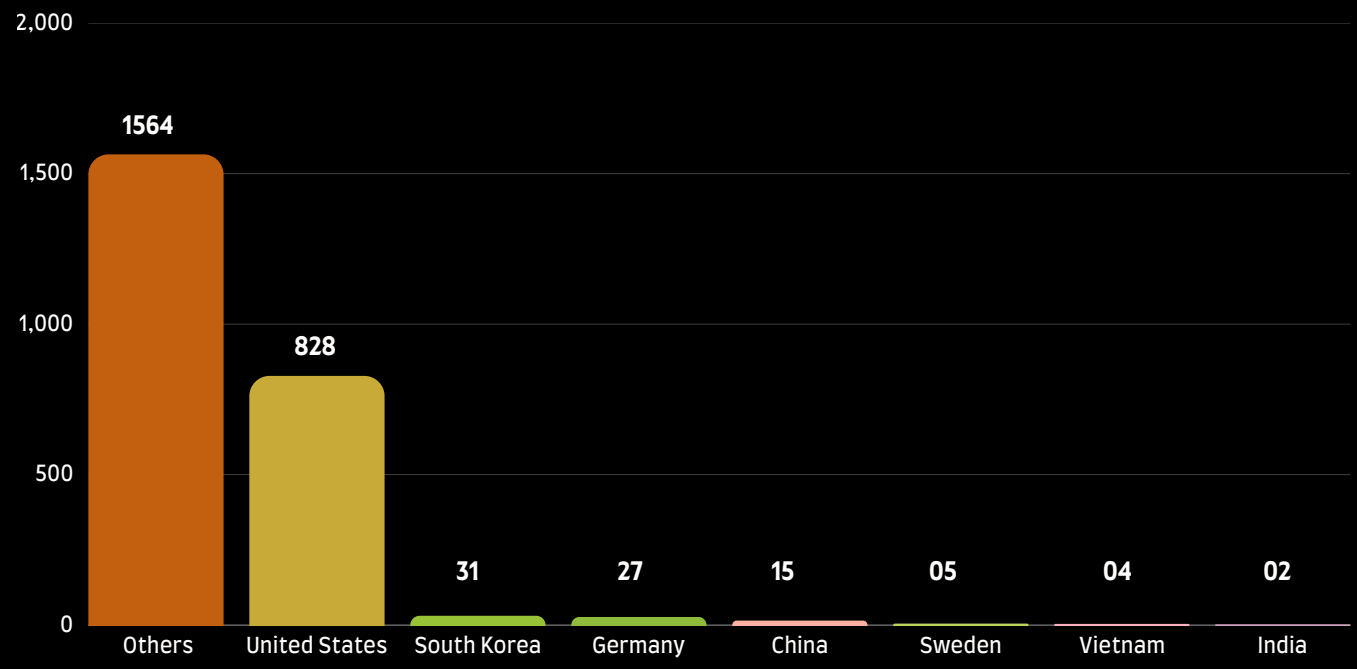
CVE ID	CVSS Score	Severity
CVE-2026-35431	10.0	Critical
CVE-2024-13152	10.0	Critical
CVE-2026-45131	10.0	Critical
CVE-2026-7312	10.0	Critical
CVE-2025-5243	10.0	Critical
CVE-2026-49777	10.0	Critical

KEY HIGHLIGHTS

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

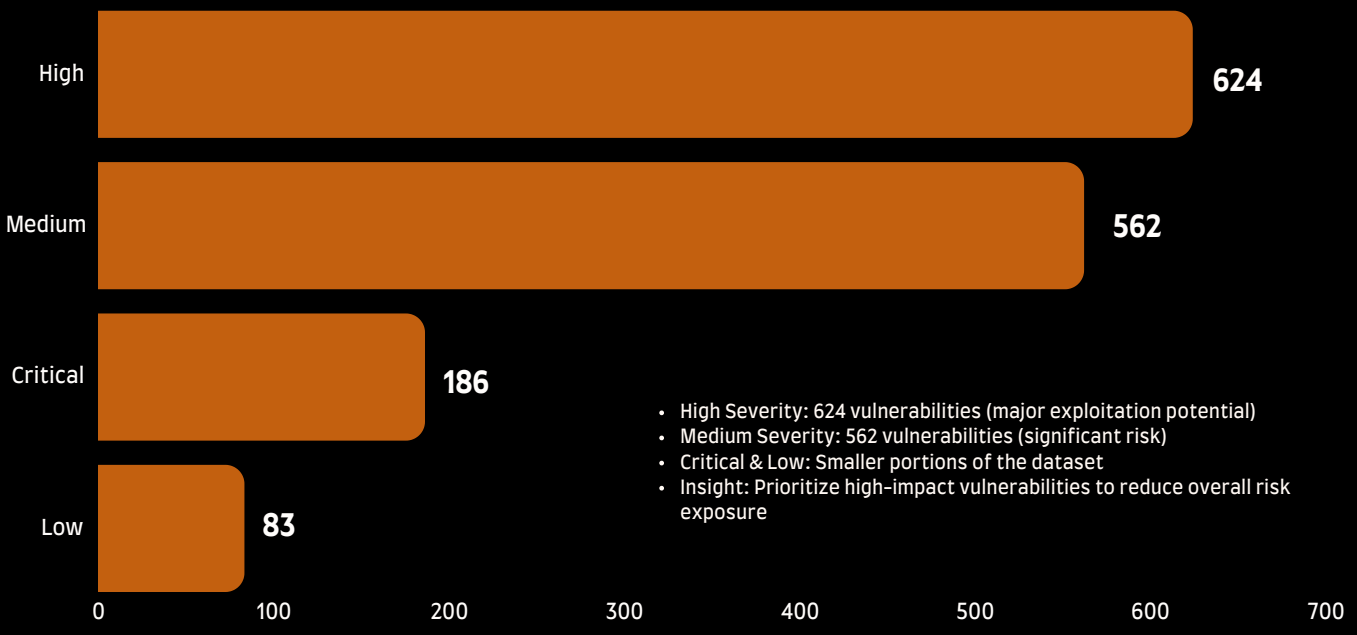
+91 7842046995 reach@castellumlabs.com www.castellumlabbs.com

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: 624 vulnerabilities (major exploitation potential)
- Medium Severity: 562 vulnerabilities (significant risk)
- Critical & Low: Smaller portions of the dataset
- Insight: Prioritize high-impact vulnerabilities to reduce overall risk exposure

Most CVEs (80%) have fixes available, but 20% remain unpatched, emphasizing the ongoing risk and the importance of timely patching.

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

CVE-2026-35431

Overview

A critical vulnerability has been identified in Microsoft Entra that allows attackers to perform spoofing attacks through a Server-Side Request Forgery (SSRF) flaw. The vulnerability affects Microsoft Entra ID Entitlement Management and can be exploited remotely without authentication.

Technical Details

The vulnerability is caused by improper handling of server-side requests, allowing attackers to force the service to send unintended requests on their behalf. By exploiting this SSRF flaw, an attacker may perform spoofing attacks against internal or trusted resources accessible to the service.

Vendor: **Microsoft**
Affected Product: **Microsoft Entra**
Affected Versions: **Not Available**

- **Published Date:** 23-04-2026
- **Last Patch:** 01-06-2026
- **Vulnerability Type:** Server-Side Request Forgery (SSRF) / Spoofing
- **Fix Available:** Yes
- **Patched Version:** Not Available

Exploitaion Status

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

Reference: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-35431

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

CVE-2024-13152

Overview

A critical vulnerability has been identified in Mobuy Online Machinery Monitoring Panel that allows attackers to execute SQL injection attacks remotely. Successful exploitation could enable unauthorized access to database contents, modification of records, or complete compromise of the application.

Technical Details

The vulnerability is caused by improper neutralization of user-supplied input before it is incorporated into SQL queries. An attacker can inject malicious SQL commands into application requests, potentially gaining unauthorized access to sensitive database information or altering data.

Vendor: **BSS Software**
Affected Product: **Mobuy Online Machinery Monitoring Panel**
Affected Versions: **Before 2.0**

- **Published Date:** 14-02-2025
- **Last Patch:** 01-06-2026
- **Vulnerability Type:** SQL Injection
- **Fix Available:** Yes
- **Patched Version:** 2.0

Exploitation Status

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

Reference: https://siberguvenlik.gov.tr/guvenlik-bildirimleri/detay/tr-25-0033

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

CVE-2026-45131

Overview

A critical vulnerability has been identified in CloudPirates Open Source Helm Charts that allows attackers to execute malicious code through GitHub Actions workflows. The flaw can expose repository secrets, including credentials and tokens, by abusing pull requests from forked repositories.

Technical Details

The vulnerability exists because the pull_request_target GitHub Actions workflow executes attacker-controlled code from forked pull requests in a privileged context. An attacker can exploit this behavior to access repository secrets, including Docker Hub credentials and authentication tokens, without requiring maintainer approval.

Affected Product: **helm-charts**
Affected Versions: **Before commit fcf930211604652aec15085895b6457bc8b73b54**
Vendor: **CloudPirates-io**

- **Published Date:** 01-06-2026
- **Last Patch:** 01-06-2026
- **Vulnerability Type:** Code Injection / Secret Exposure
- **Fix Available:** Yes
- **Patched Version:** fcf930211604652aec15085895b6457bc8b73b54

Exploitation Status

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

Reference: https://github.com/CloudPirates-io/helm-charts/security/advisories/GHSA-c47r-c7gw-cvph

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

CVE-2026-7312

Overview

A critical vulnerability has been identified in Sitefinity that may expose plaintext credentials used to connect to the Sitefinity Insight service. An unauthenticated remote attacker could obtain these credentials when specific integrations and non-default configurations are in use.

Technical Details

The vulnerability stems from insufficient protection of credentials within Sitefinity web services. A remote attacker can obtain plaintext credentials used for Sitefinity Insight integration, potentially leading to unauthorized access to connected services.

Affected Product: **Sitefinity**
Affected Versions: **14.0.7700 before 14.4.8152 , 15.0.8200 before 15.0.8234**
Vendor: **Progress Software**

- **Published Date:** 02-06-2026
- **Last Patch:** 02-06-2026
- **Vulnerability Type:** Insufficiently Protected Credentials / Credential Exposure
- **Fix Available:** Yes
- **Patched Version:** 14.4.8152, 15.0.8234, 15.1.8335, 15.2.8441, 15.3.8531, 15.4.8630

Exploitation Status

- Exploited in the Wild: No known exploitation
- Threat Actors / Malware: None reported
- Exploit Availability: no confirmed public PoC observed

Reference: https://community.progress.com/s/article/Sitefinity-Security-Advisory-for-Addressing-Security-Vulnerabilities-CVE-2026-7312-CVE-2026-7198-CVE-2026-7195-CVE-2026-7201-CVE-2026-7313-May-2026

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

CVE-2025-5243

Overview

A critical vulnerability has been identified in Information Portal that allows attackers to upload malicious files and execute arbitrary commands on the server. Successful exploitation can lead to web shell deployment, remote code execution, and complete compromise of the affected application.

Technical Details

The vulnerability is caused by unrestricted file upload functionality combined with improper neutralization of operating system commands. An attacker can upload malicious files such as web shells and leverage command injection techniques to execute arbitrary code on the underlying server.

Affected Product: **Information Portal**
Affected Versions: **Before 13.06.2025**
Vendor: **SMG Software**

- **Published Date:** 24-07-2025
- **Last Patch:** 05-06-2026
- **Vulnerability Type:** Arbitrary File Upload / OS Command Injection / Remote Code Execution
- **Fix Available:** Yes
- **Patched Version:** 13.06.2025

Exploitation Status

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

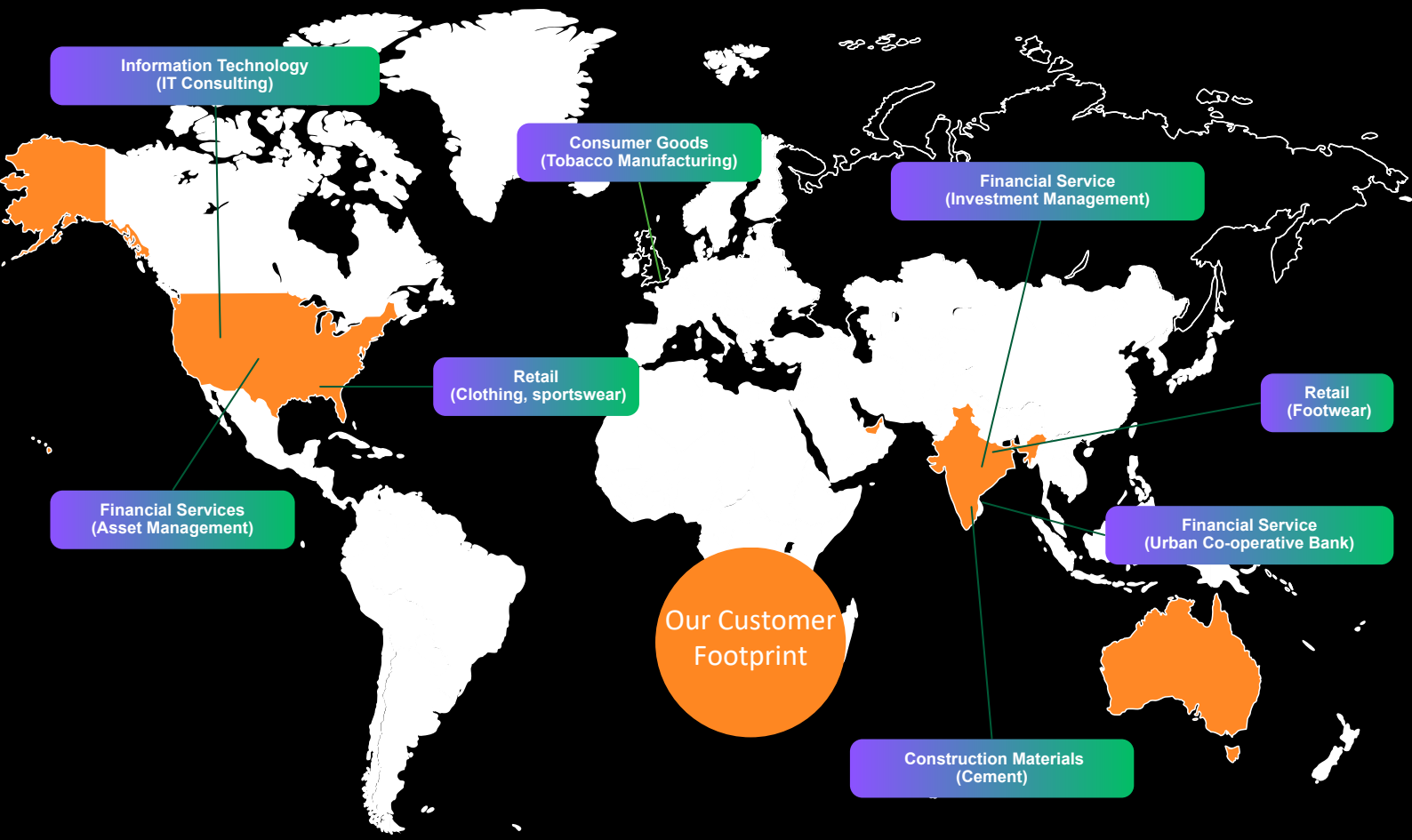
Reference: https://www.usom.gov.tr/bildirim/tr-25-0174

+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