CASTELLUM LABS

WEEKLY DIGEST

VULNERABILITIES

Reporting Period – 19 Apr – 02 MAY

enisa | EUROPEAN UNION VULNERABILITY DATABASE

NIST CVE

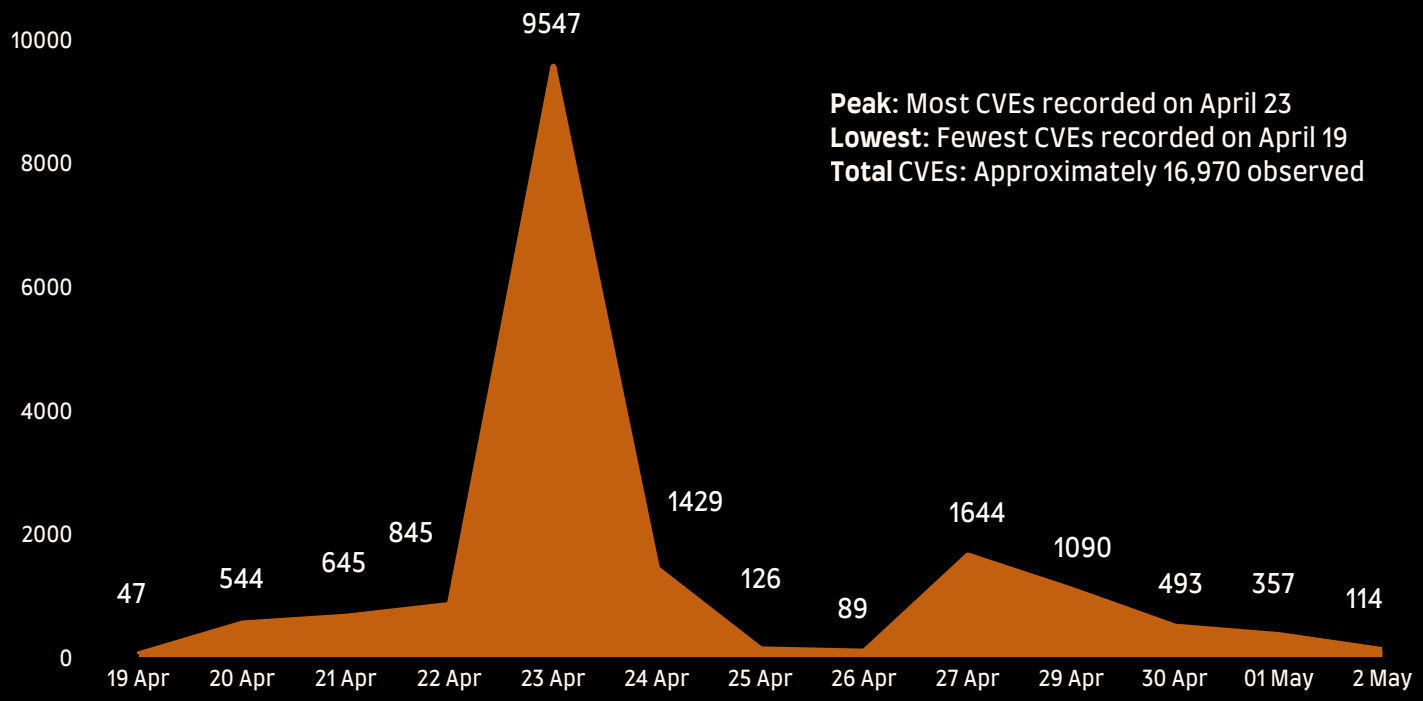
OSV

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

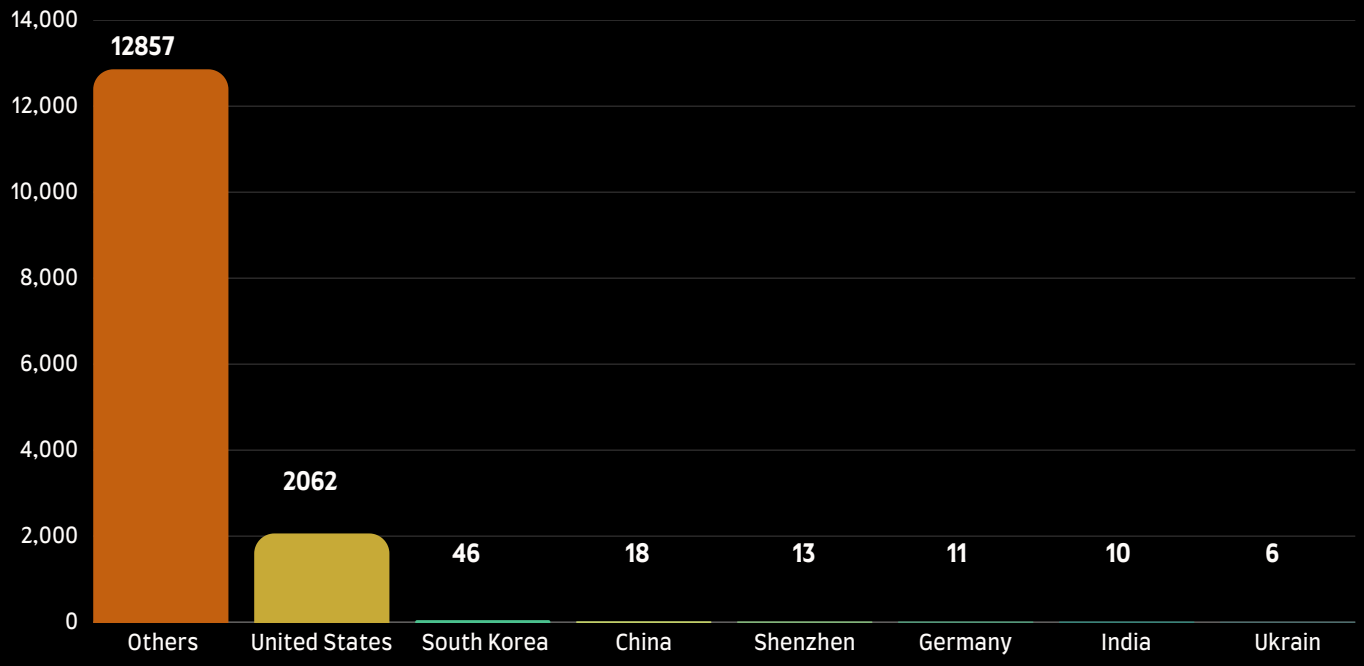
CVE ID	CVSS Score	Severity
CVE-2026-41228	10.0	Critical
CVE-2025-22654	10.0	Critical
CVE-2025-26936	10.0	Critical
CVE-2026-42778	10.0	Critical
CVE-2026-33819	10.0	Critical
CVE-2025-53577	10.0	Critical

KEY HIGHLIGHTS

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

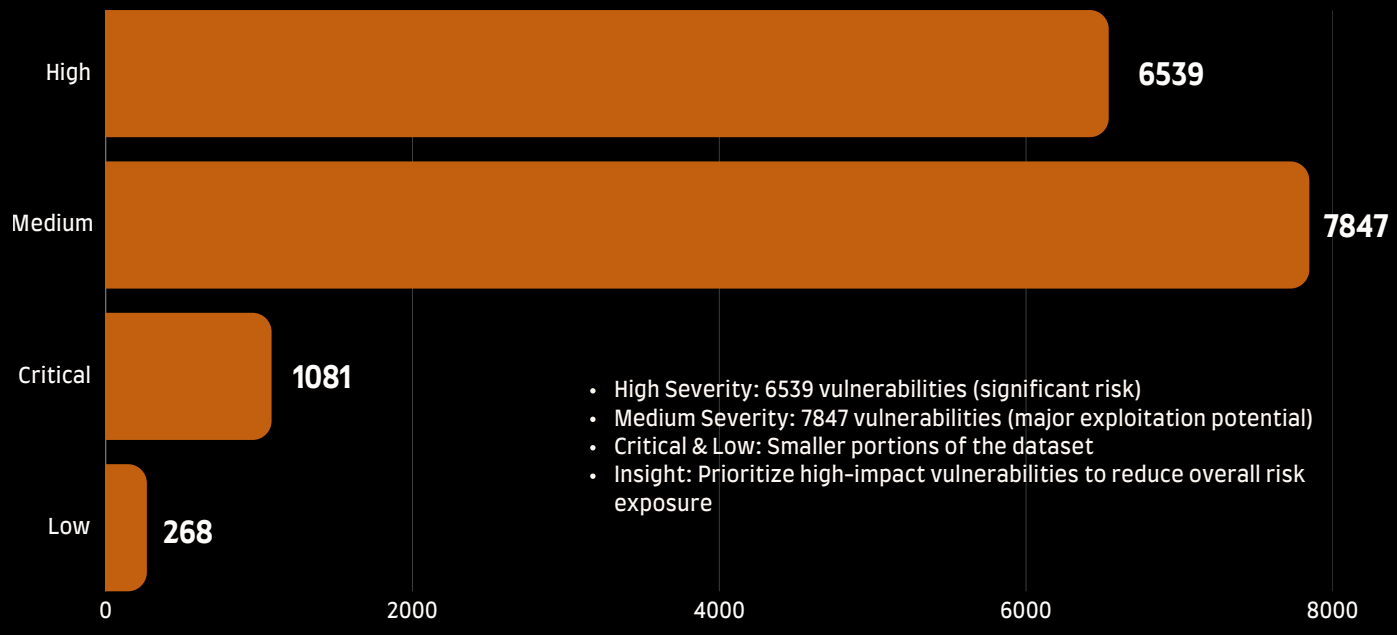
+91 7842046995 reach@castellumlabs.com www.castellumlabbs.com

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: 6539 vulnerabilities (significant risk)
- Medium Severity: 7847 vulnerabilities (major exploitation potential)
- Critical & Low: Smaller portions of the dataset
- Insight: Prioritize high-impact vulnerabilities to reduce overall risk exposure

Most CVEs (92.4%) have fixes available, but 7.6 % remain unpatched, emphasizing the ongoing risk and the importance of timely patching.

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

CVE-2026-41228

Overview

A critical vulnerability in Froxlor affects versions before 2.3.6, allowing authenticated users to achieve remote code execution via the API.

Technical Details

The def_language parameter in Customers.update and Admins.update allows path traversal, enabling attackers to load malicious PHP files and execute code.

Vendor: Froxlor
Affected Product: Froxlor
Affected Versions: Before 2.3.6

- **Published Date:** 23-04-2026
- **Last Patch:** 23-04-2026
- **Vulnerability Type:** Local File Inclusion / Remote Code Execution
- **Fix Available:** Yes
- **Patched Version:** 2.3.6

Exploitaion Status

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

Reference: github.com: https://github.com/froxlor/froxlor/security/advisories/GHSA-w59f-67xm-rxx7

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

CVE-2025-22654

Overview

A critical vulnerability in Simplified allows attackers to upload malicious files, potentially leading to server compromise.

Technical Details

The plugin allows unrestricted upload of dangerous file types, enabling arbitrary file upload.

Vendor: kodeshpa
Affected Product: Simplified
Affected Versions: 0 through 1.0.6

- **Published Date:** 18-02-2025
- **Last Patch:** 28-04-2026
- **Vulnerability Type:** Arbitrary File Upload
- **Fix Available:** Yes
- **Patched Version:** 1.0.7

Exploitation Status

- Exploited in the Wild: No known exploitation
- Threat Actors / Malware: None reported
- Exploit Availability: Public PoC reported on security tracking platform

Reference:
https://patchstack.com/database/Wordpress/Plugin/simplified/vulnerability/wordpress-simplified-plugin-plugin-1-0-6-arbitrary-file-upload-vulnerability?_s_id=cve

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

CVE-2025-26936

Overview

A critical vulnerability in Fresh Framework allows unauthenticated remote code execution through code injection.

Technical Details

The plugin improperly handles user input, allowing attackers to inject and execute malicious code without authentication.

Affected Product: Fresh Framework
Affected Versions: 0 through 1.70.0
Vendor: FRESHFACE

- **Published Date:** 10-03-2025
- **Last Patch:** 28-04-2026
- **Vulnerability Type:** Code Injection / Remote Code Execution
- **Fix Available:** Yes
- **Patched Version:** Not Available

Exploitation Status

- Exploited in the Wild: No known exploitation
- Threat Actors / Malware: None reported
- Exploit Availability: Not publicly observed

Reference: https://patchstack.com/database/Wordpress/Plugin/fresh-framework/vulnerability/wordpress-fresh-framework-plugin-1-70-0-unauthenticated-remote-code-execution-rce-vulnerability?_s_id=cve

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

CVE-2026-42778

Overview

A critical vulnerability in Apache MINA affects certain 2.1.x and 2.2.x versions due to an incomplete fix for a previous deserialization flaw. Successful exploitation may allow remote attackers to execute arbitrary code in applications using IoBuffer.getObject().

Technical Details

The earlier security fix applied the class allowlist too late, after class initialization could already occur during deserialization. Attackers can exploit crafted serialized objects to trigger unsafe code execution in vulnerable Apache MINA applications.

Affected Product: Apache MINA
Affected Versions: 2.1.X through 2.1.11, 2.2.X through 2.2.6
Vendor: Apache Software Foundation

- **Published Date:** 01-05-2026
- **Last Patch:** 01-05-2026
- **Vulnerability Type:** Deserialization of Untrusted Data / Remote Code Execution
- **Fix Available:** Yes
- **Patched Version:** 2.1.12, 2.2.7

Exploitation Status

- Exploited in the Wild: No known exploitation
- Threat Actors / Malware: None reported
- Exploit Availability: Not publicly observed

Reference: https://lists.apache.org/thread/fhlx5k91hrkgyzh7yk1nghrn3k27gxy0

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

CVE-2026-33819

Overview

A critical vulnerability has been identified in Microsoft Bing that could allow unauthorized remote code execution over a network. The issue affects Microsoft's hosted Bing service and is caused by insecure handling of untrusted serialized data.

Technical Details

The vulnerability is caused by deserialization of untrusted data, where crafted input may be processed insecurely by the Bing service. An attacker can exploit this remotely without authentication to potentially execute arbitrary code on the affected service.

Affected Product: Microsoft Bing
Affected Versions: Not Available
Vendor: Microsoft

- **Published Date:** 23-04-2026
- **Last Patch:** 11-05-2026
- **Vulnerability Type:** Deserialization of Untrusted Data / Remote Code Execution
- **Fix Available:** Yes
- **Patched Version:** Not Available

Exploitation Status

- Exploited in the Wild: No known exploitation
- Threat Actors / Malware: None reported
- Exploit Availability: Not publicly observed

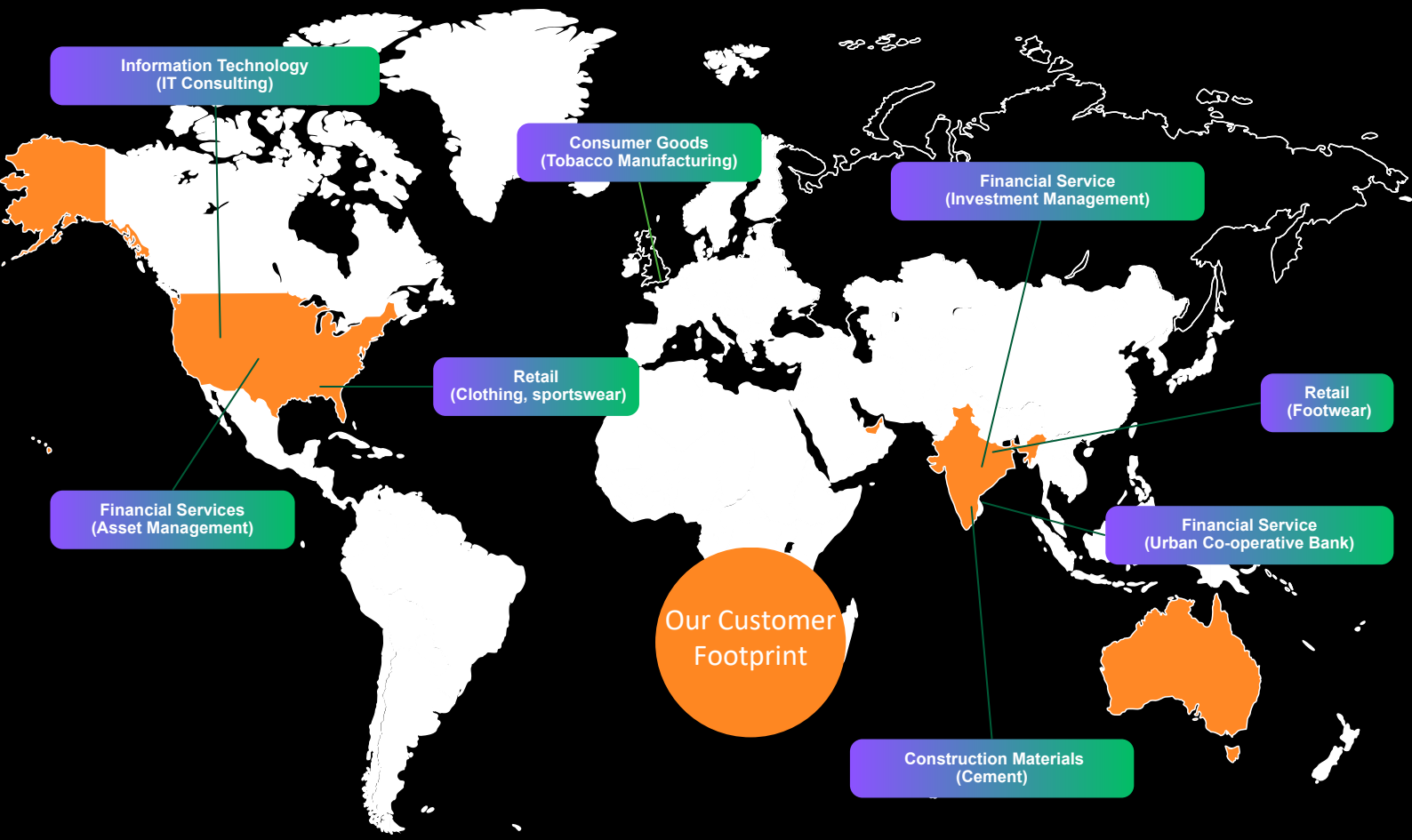
Reference: msrc.microsoft.com: Microsoft Bing Remote Code Execution Vulnerability

+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