CASTELLUM LABS

WEEKLY DIGEST

VULNERABILITIES

Reporting Period – 17 MAY – 23 MAY 2026

enisa EUROPEAN UNION VULNERABILITY DATABASE

NIST CVE

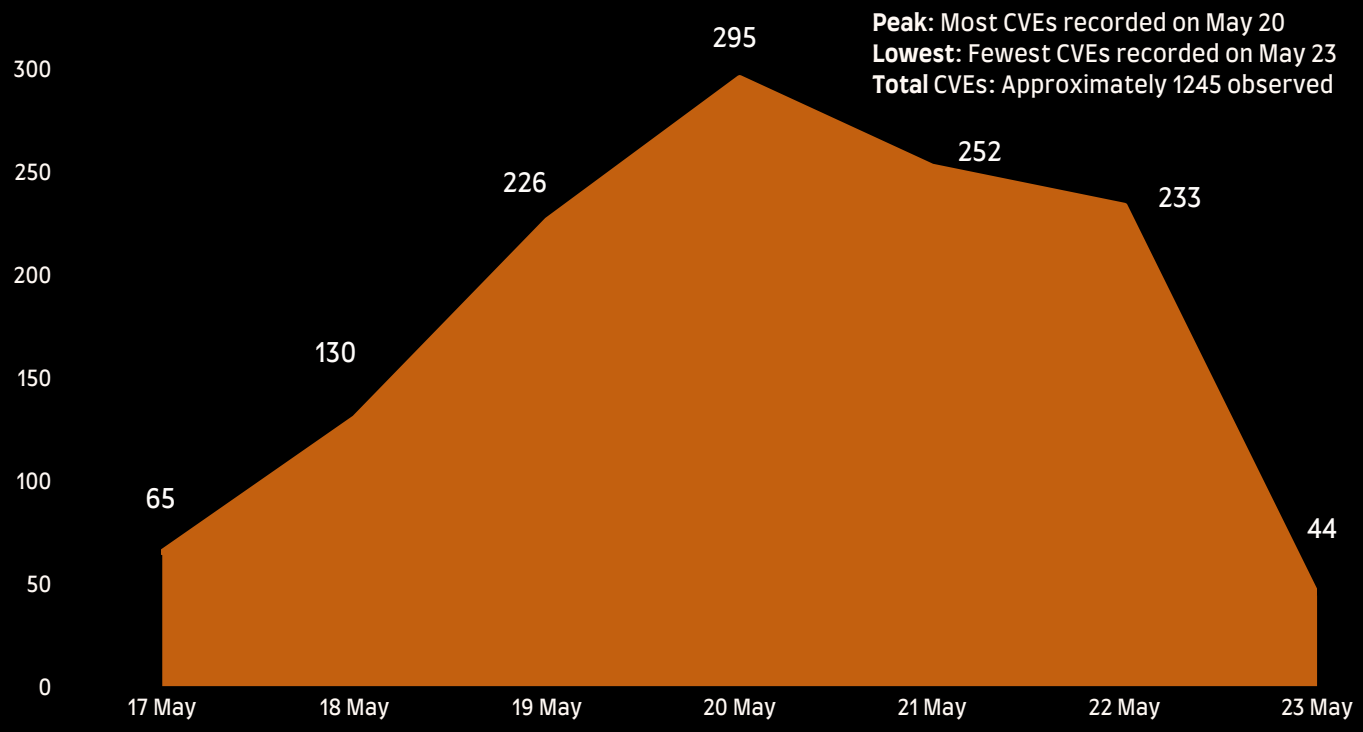
OSV

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

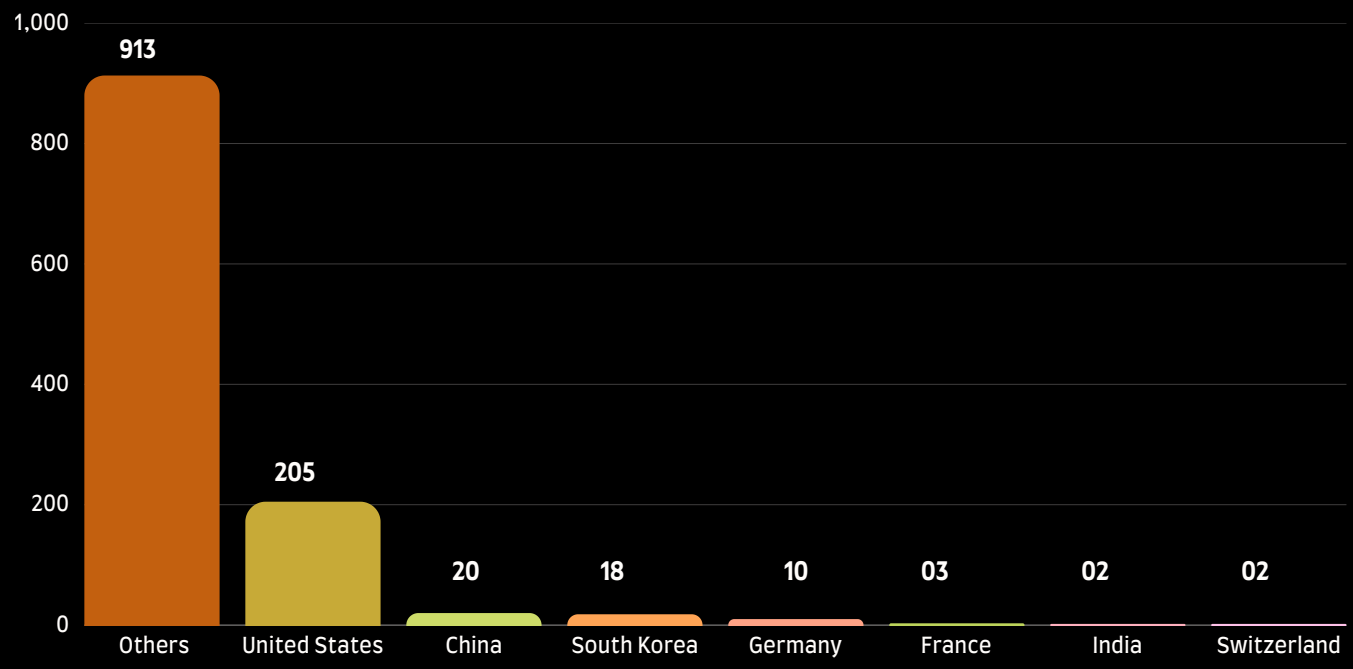
CVE ID	CVSS Score	Severity
CVE-2026-42822	10.0	Critical
CVE-2026-43633	10.0	Critical
CVE-2026-20223	10.0	Critical
CVE-2026-34910	10.0	Critical
CVE-2026-45444	10.0	Critical
CVE-2026-23652	10.0	Critical

KEY HIGHLIGHTS

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

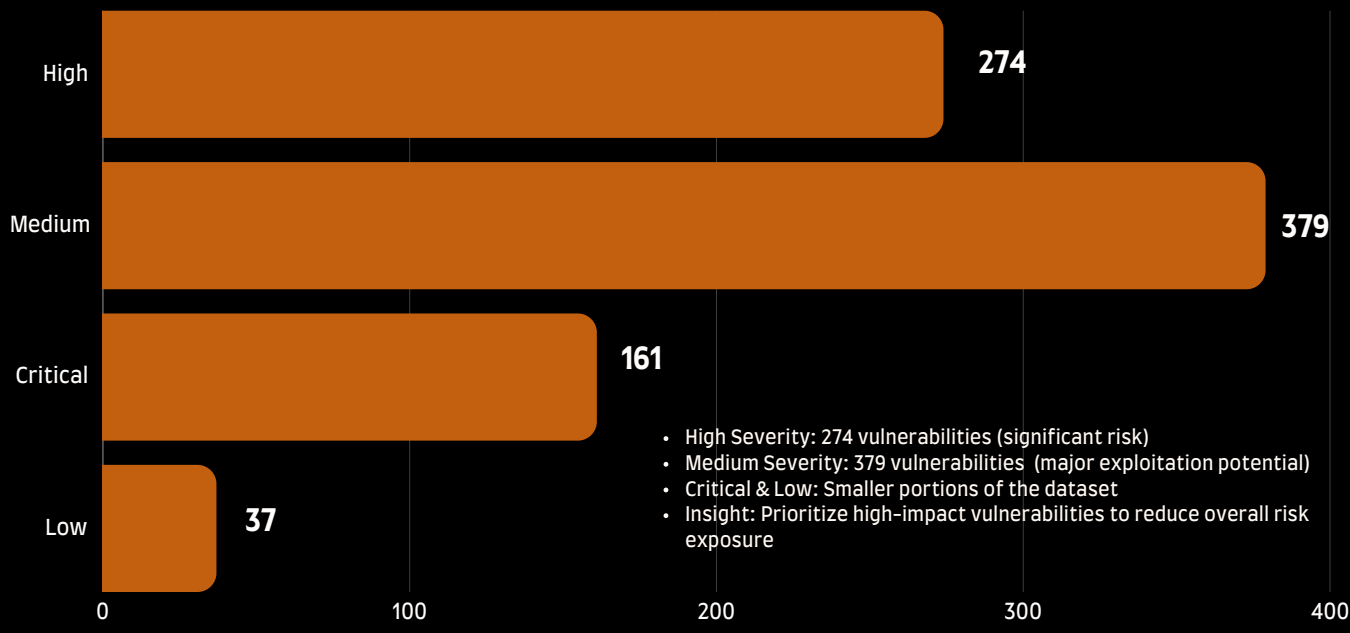
+91 7842046995 reach@castellumlabs.com www.castellumlabbs.com

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



Most CVEs (82.9%) have fixes available, but 17.1% remain unpatched, emphasizing the ongoing risk and the importance of timely patching.

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

CVE-2026-42822

Overview

A critical vulnerability has been identified in Azure Local that could allow unauthorized attackers to elevate privileges over a network. The issue affects Azure Local Disconnected Operations (ALDO) due to improper authentication handling.

Technical Details

The vulnerability is caused by improper authentication mechanisms within Azure Local Disconnected Operations. An attacker can exploit the flaw remotely to gain elevated privileges on the affected system without valid authorization.

Vendor: Microsoft
Affected Product: Azure Local
Affected Versions: 1.0.0 before 2604.2.25645

- **Published Date:** 18-05-2026
- **Last Patch:** 22-05-2026
- **Vulnerability Type:** Improper Authentication / Elevation of Privilege
- **Fix Available:** Yes
- **Patched Version:** 2604.2.25645

Exploitaion Status

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

Reference: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42822

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

CVE-2026-43633

Overview

A critical vulnerability has been identified in HestiaCP that allows unauthenticated remote attackers to achieve root-level remote code execution. The issue affects the web terminal component due to insecure deserialization between PHP and Node.js session handling.

Technical Details

The vulnerability is caused by a session format mismatch where attacker-controlled HTTP header data is processed differently by PHP and Node.js components. An attacker can inject crafted serialized session values that are trusted by the web terminal service, resulting in arbitrary command execution as root.

Vendor: hestiacp
Affected Product: hestiacp
Affected Versions: 1.9.0 through 1.9.4

- **Published Date:** 19-05-2026
- **Last Patch:** 19-05-2026
- **Vulnerability Type:** Deserialization of Untrusted Data / Remote Code Execution
- **Fix Available:** Yes
- **Patched Version:** 854d71b3c1737b0a0d0cc55c926008ffe1f6719b

Exploitation Status

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

Reference:
https://github.com/hestiacp/hestiacp/commit/854d71b3c1737b0a0d0cc55c926008ffe1f6719b

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

CVE-2026-20223

Overview

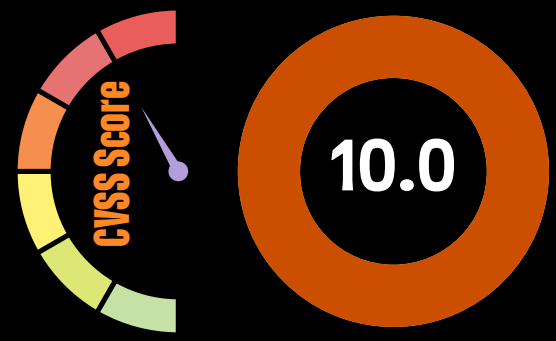
A critical vulnerability has been identified in Cisco Secure Workload that allows unauthenticated remote attackers to gain Site Admin privileges through internal REST APIs. Successful exploitation could allow attackers to access sensitive information and modify configurations across tenant boundaries.

Technical Details

The vulnerability is caused by insufficient validation and missing authentication checks in internal REST API endpoints. An attacker can send crafted API requests to bypass access controls and gain Site Admin privileges without authentication.

Affected Product: Cisco Secure Workload
Affected Versions: Multiple versions from 1.102.21 through 4.0.3.13
Vendor: Cisco

- **Published Date:** 20-05-2026
- **Last Patch:** 20-05-2026
- **Vulnerability Type:** Missing Authentication for Critical Function / Unauthorized API Access
- **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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-csw-pnbsa-g8WEnuy

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

CVE-2026-34910

Overview

A critical vulnerability has been identified in multiple UniFi OS Server devices that could allow remote attackers to execute arbitrary commands. The issue is caused by improper input validation and may lead to command injection on affected UniFi OS systems.

Technical Details

The vulnerability is caused by improper validation of user-supplied input processed by UniFi OS devices. A remote attacker with network access can exploit the flaw to inject and execute arbitrary commands on vulnerable systems.

Affected Product: Multiple products UniFi OS Server
Affected Versions: Multiple products before versions 5.0.8, 5.1.10, 5.1.11, and 5.1.12
Vendor: Ubiquiti Inc

- **Published Date:** 22-05-2026
- **Last Patch:** 22-05-2026
- **Vulnerability Type:** Improper Input Validation / Command Injection
- **Fix Available:** Yes
- **Patched Version:** 5.0.8, 5.1.10, 5.1.11, 5.1.12 (depending on product)

Exploitation Status

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

Reference: https://community.ui.com/releases/Security-Advisory-Bulletin-064-064/84811c09-4cf4-42ab-bd61-cc994445963b

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

CVE-2026-45444

Overview

A critical vulnerability has been identified in Gift Cards For WooCommerce Pro that allows attackers to upload malicious files to the server. Successful exploitation may lead to remote code execution and complete compromise of affected WordPress installations.

Technical Details

The vulnerability is caused by unrestricted upload of dangerous file types without proper validation or filtering. An attacker can upload malicious files to the server and potentially execute arbitrary code on the affected system.

Affected Product: **Gift Cards For WooCommerce Pro**
Affected Versions: **Through 4.2.6**
Vendor: **WP Swings**

- **Published Date:** 20-05-2026
- **Last Patch:** 20-05-2026
- **Vulnerability Type:** Arbitrary File Upload / Unrestricted Upload of File with Dangerous Type
- **Fix Available:** Yes
- **Patched Version:** Not Available

Exploitation Status

- Exploited in the Wild: known exploitation
- Threat Actors / Malware: None reported
- Exploit Availability: Public advisory available

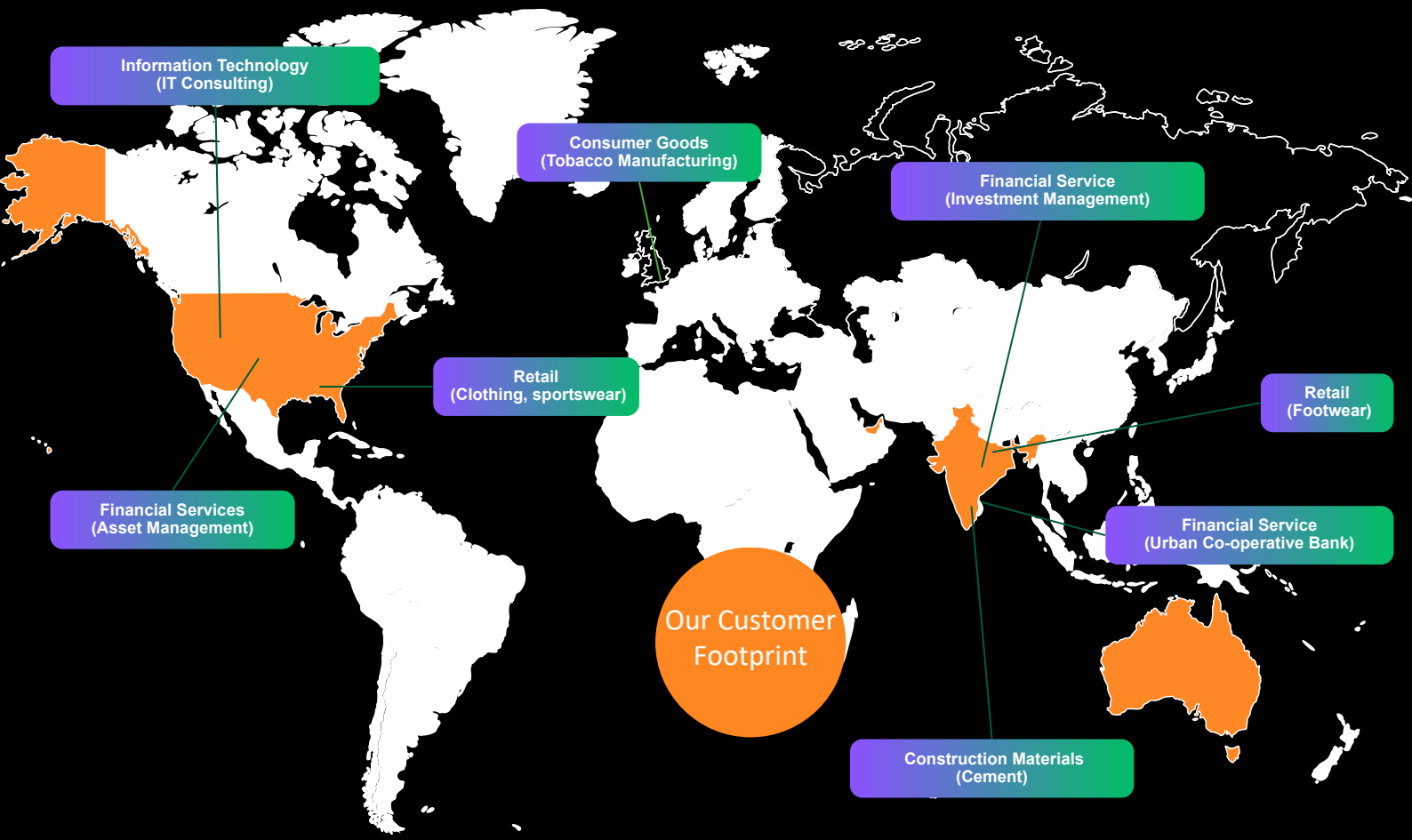
Reference: https://patchstack.com/database/wordpress/plugin/giftware/vulnerability/wordpress-gift-cards-for-woocommerce-pro-plugin-4-2-6-arbitrary-file-upload-vulnerability?_s_id=cve

+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