CASTELLUM LABS

WEEKLY DIGEST

VULNERABILITIES

Reporting Period – 24 MAY – 30 MAY 2026

enisa EUROPEAN UNION VULNERABILITY DATABASE

NIST CVE

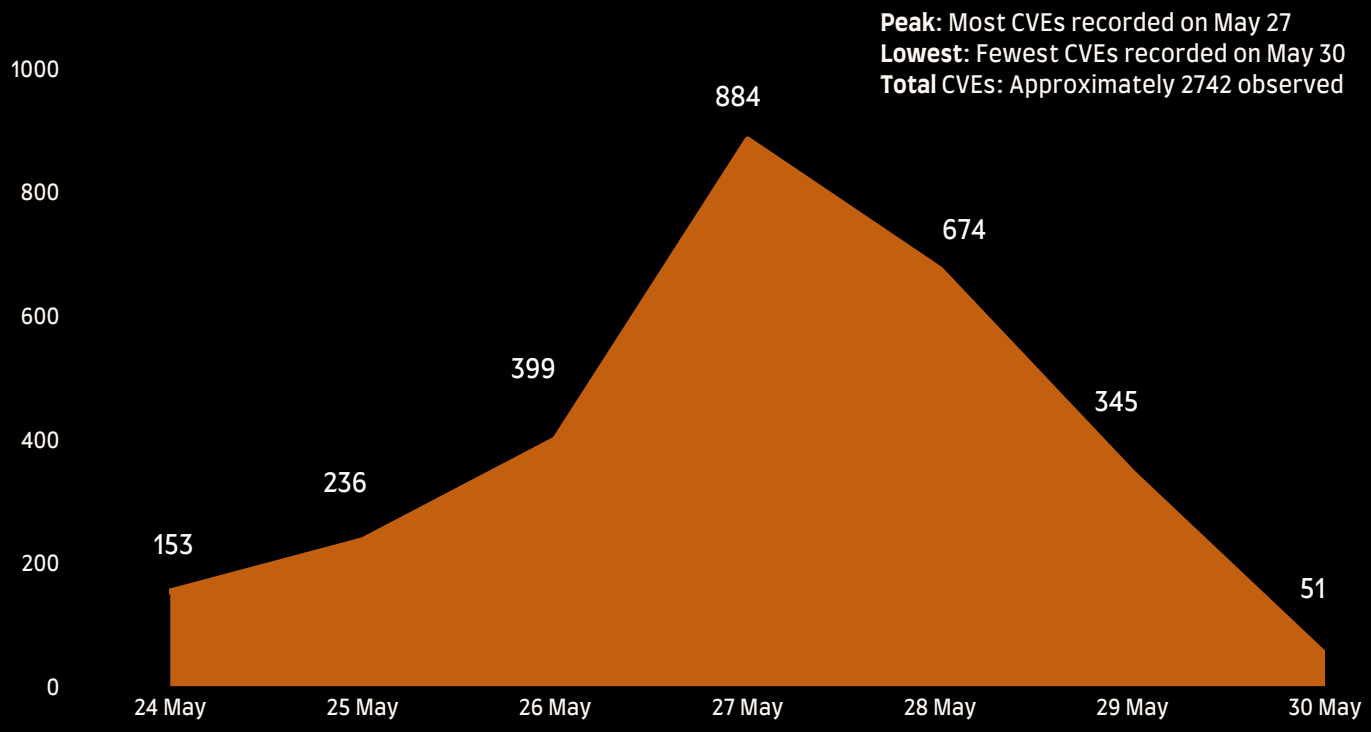
OSV

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

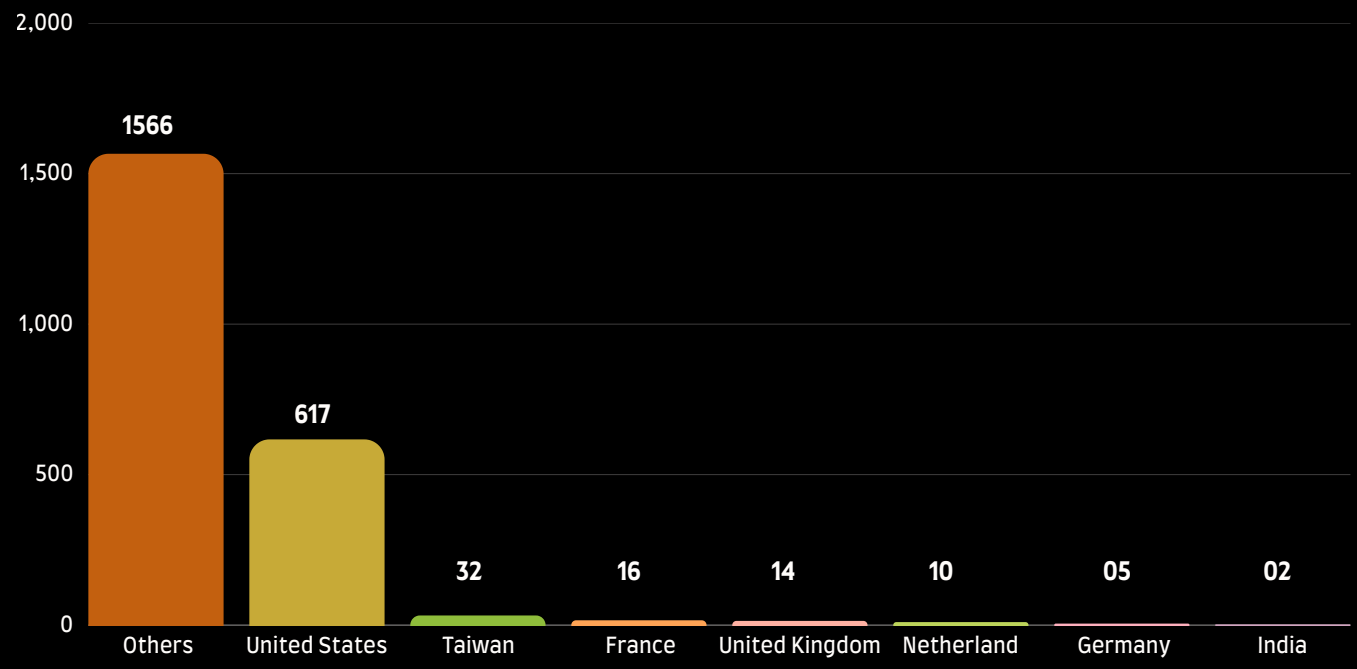
CVE ID	CVSS Score	Severity
CVE-2023-7028	10.0	Critical
CVE-2026-44330	10.0	Critical
CVE-2026-46840	10.0	Critical
CVE-2026-44962	10.0	Critical
CVE-2026-45631	10.0	Critical
CVE-2026-45087	10.0	Critical

KEY HIGHLIGHTS

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

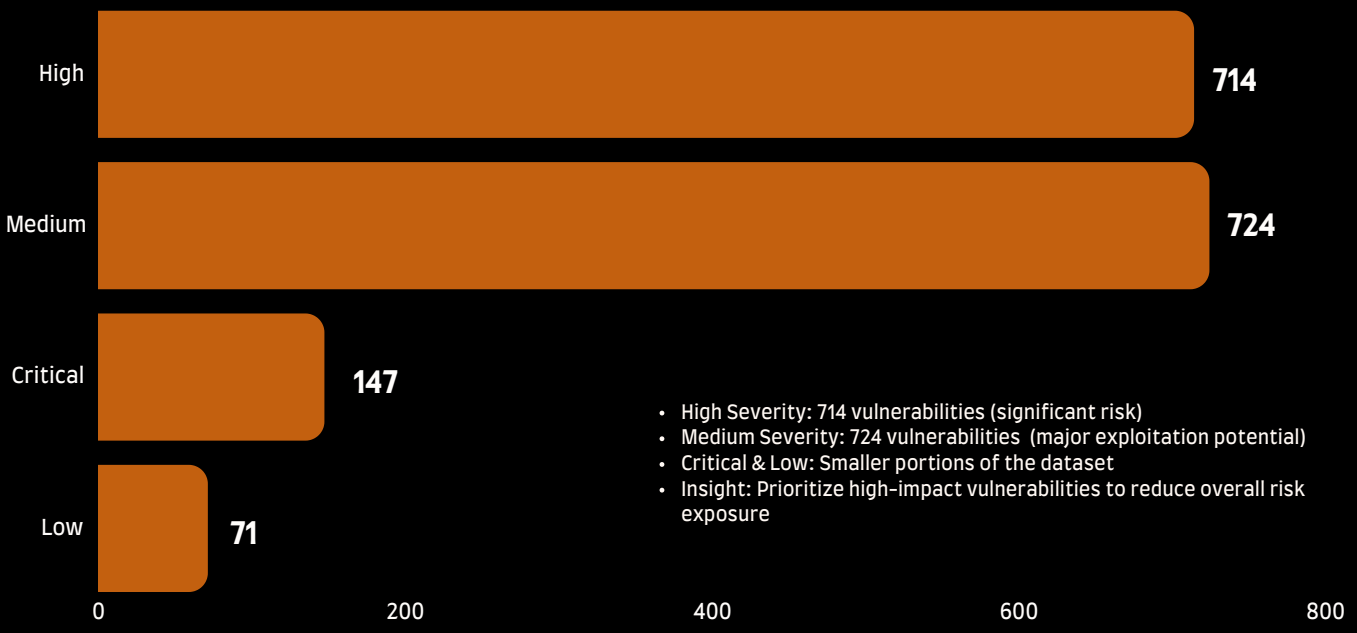
+91 7842046995 reach@castellumlabs.com www.castellumlabbs.com

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: 714 vulnerabilities (significant risk)
- Medium Severity: 724 vulnerabilities (major exploitation potential)
- Critical & Low: Smaller portions of the dataset
- Insight: Prioritize high-impact vulnerabilities to reduce overall risk exposure

Most CVEs (74.8%) have fixes available, but 25.2% remain unpatched, emphasizing the ongoing risk and the importance of timely patching.

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

CVE-2023-7028

Overview

A critical vulnerability has been identified in GitLab that could allow password reset emails to be sent to unverified email addresses. This weakness in the password recovery mechanism may enable attackers to take over user accounts under certain conditions.

Technical Details

The vulnerability exists because password reset emails could be delivered to email addresses that had not been verified by the account owner. An attacker may exploit this flaw to receive password reset links and potentially gain unauthorized access to affected accounts.

Vendor: **GitLab**
Affected Product: **GitLab CE/EE**
Affected Versions: **16.1 before 16.1.6**

- **Published Date:** 12-01-2024
- **Last Patch:** 26-05-2026
- **Vulnerability Type:** Weak Password Recovery Mechanism for Forgotten Password / Account Takeover
- **Fix Available:** Yes
- **Patched Version:** 16.1.6, 16.2.9, 16.3.7, 16.4.5, 16.5.6, 16.6.4, 16.7.2

Exploitaion Status

- Exploited in the Wild: known exploitation
- Threat Actors / Malware: None reported
- Exploit Availability: Public exploit details available through disclosed security research

Reference: https://hackerone.com/reports/2293343

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

CVE-2026-44330

Overview

A critical vulnerability has been identified in free5GC that allows unauthenticated access to the NEF nnef-pfdmanagement API. An attacker can use forged bearer tokens to access PFD data and manage subscriptions without proper authorization.

Technical Details

The vulnerability exists because the nnef-pfdmanagement route group is deployed without OAuth2 or bearer-token authorization middleware. A remote attacker can send arbitrary bearer tokens to read PFD application data and create or delete PFD notification subscriptions.

Vendor: **free5gc**
Affected Product: **free5GC**
Affected Versions: **Before 4.2.2**

- **Published Date:** 27-05-2026
- **Last Patch:** 27-05-2026
- **Vulnerability Type:** Incorrect Authorization / Authentication Bypass
- **Fix Available:** Yes
- **Patched Version:** 4.2.2

Exploitation Status

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

Reference: https://github.com/free5gc/free5gc/security/advisories/GHSA-rwww-x45w-p52w

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

CVE-2026-46840

Overview

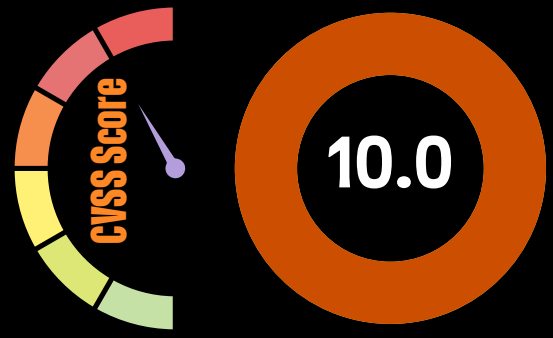
A critical vulnerability has been identified in Oracle REST Data Services that allows unauthenticated attackers to compromise affected systems over HTTPS. Successful exploitation can lead to complete takeover of Oracle REST Data Services and may impact additional connected products.

Technical Details

The vulnerability affects the Backend-as-a-Service component and can be exploited remotely by an unauthenticated attacker with HTTPS network access. A successful attack can result in full compromise of Oracle REST Data Services, impacting confidentiality, integrity, and availability.

Affected Product: **Oracle REST Data Services**
Affected Versions: **24.2.0 through 26.1.0**
Vendor: **Oracle Corporation**

- **Published Date:** 28-05-2026
- **Last Patch:** 28-05-2026
- **Vulnerability Type:** Not Available
- **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://www.oracle.com/security-alerts/cspumay2026.html

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

CVE-2026-44962

Overview

A critical vulnerability has been identified in Plesk that allows authenticated low-privileged users to execute arbitrary operating system commands. The issue exists in the APS Application Catalog search functionality and can lead to local privilege escalation on affected servers.

Technical Details

The vulnerability is caused by improper sanitization of user-supplied input that is incorporated into XPath queries within the APS Application Catalog search feature. An authenticated attacker can exploit this XPath injection flaw to execute arbitrary system commands and elevate privileges on the server.

Affected Product: **Plesk**
Affected Versions: **18.0.75.1 and 18.0.76.2 (as listed in the CVE record)**
Vendor: **WebPros**

- **Published Date:** 29-05-2026
- **Last Patch:** 29-05-2026
- **Vulnerability Type:** XPath Injection / Local Privilege Escalation
- **Fix Available:** Yes
- **Patched Version:** Not Available

Exploitation Status

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

Reference:https://support.plesk.com/hc/en-us/articles/38633651286679-Vulnerability-CVE-2026-44962-in-Plesk-s-APS-Catalog

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

CVE-2026-45631

Overview

A critical vulnerability has been identified in Dokploy that allows unauthenticated attackers to take over administrator accounts. The issue is caused by a hardcoded authentication secret that can be used to forge authentication tokens and gain full control of the platform.

Technical Details

The vulnerability stems from a hardcoded fallback BETTER_AUTH_SECRET value that is used when a custom secret is not configured. An attacker can forge email verification JWTs, automatically sign in as an administrator, and execute commands on the host through the built-in SSH terminal.

Dokploy

Affected Product: **Dokploy**
Affected Versions: **>= 0.27.0, < 0.29.3**
Vendor: **Dokploy**

- **Published Date:** 29-05-2026
- **Last Patch:** 29-05-2026
- **Vulnerability Type:** Use of Hard-coded Credentials / Authentication Bypass / Remote Code Execution
- **Fix Available:** Yes
- **Patched Version:** 0.29.3

Exploitation Status

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

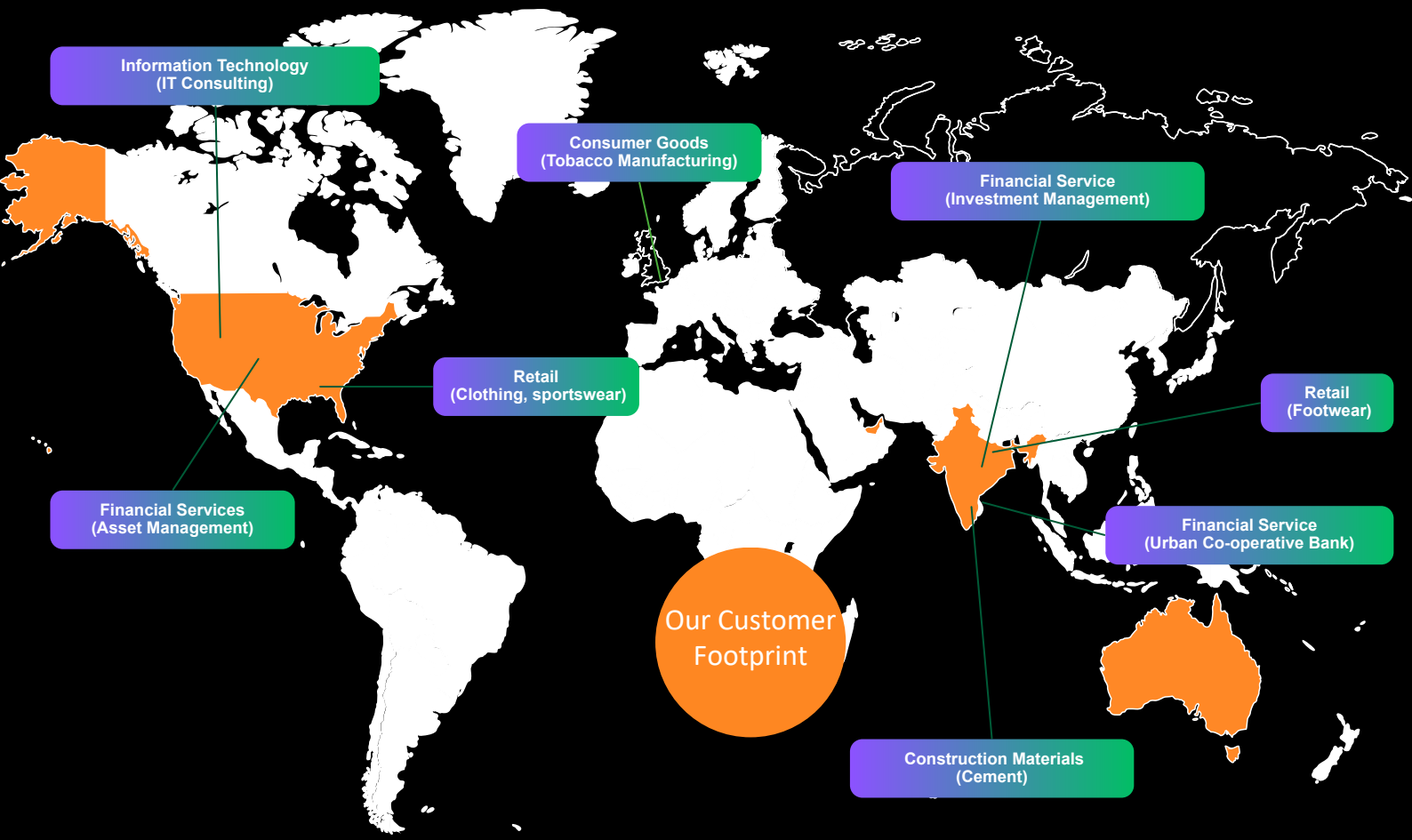
Reference: https://github.com/Dokploy/dokploy/security/advisories/GHSA-w3gm-rc4p-9rhj

+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