CASTELLUM LABS

WEEKLY DIGEST

VULNERABILITIES

Reporting Period – 03 MAY – 16 MAY 2026

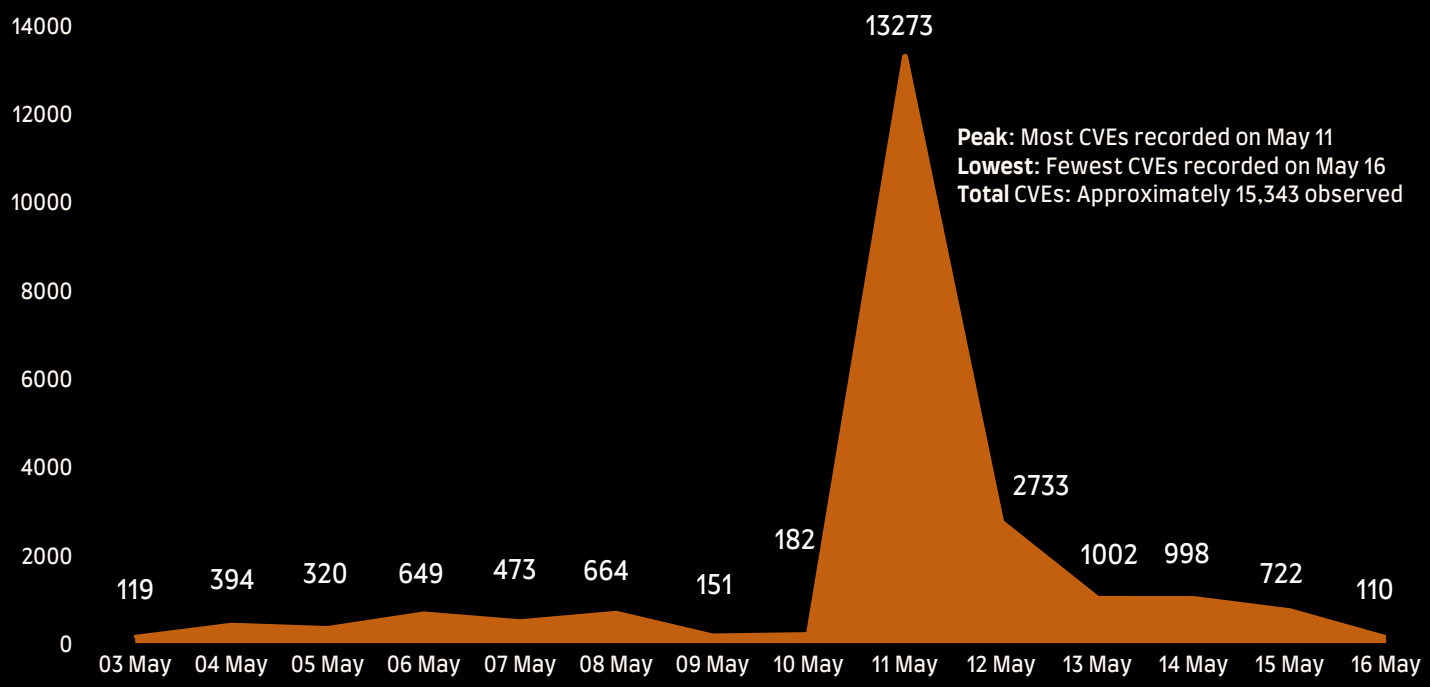
enisa EUROPEAN UNION VULNERABILITY DATABASE

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

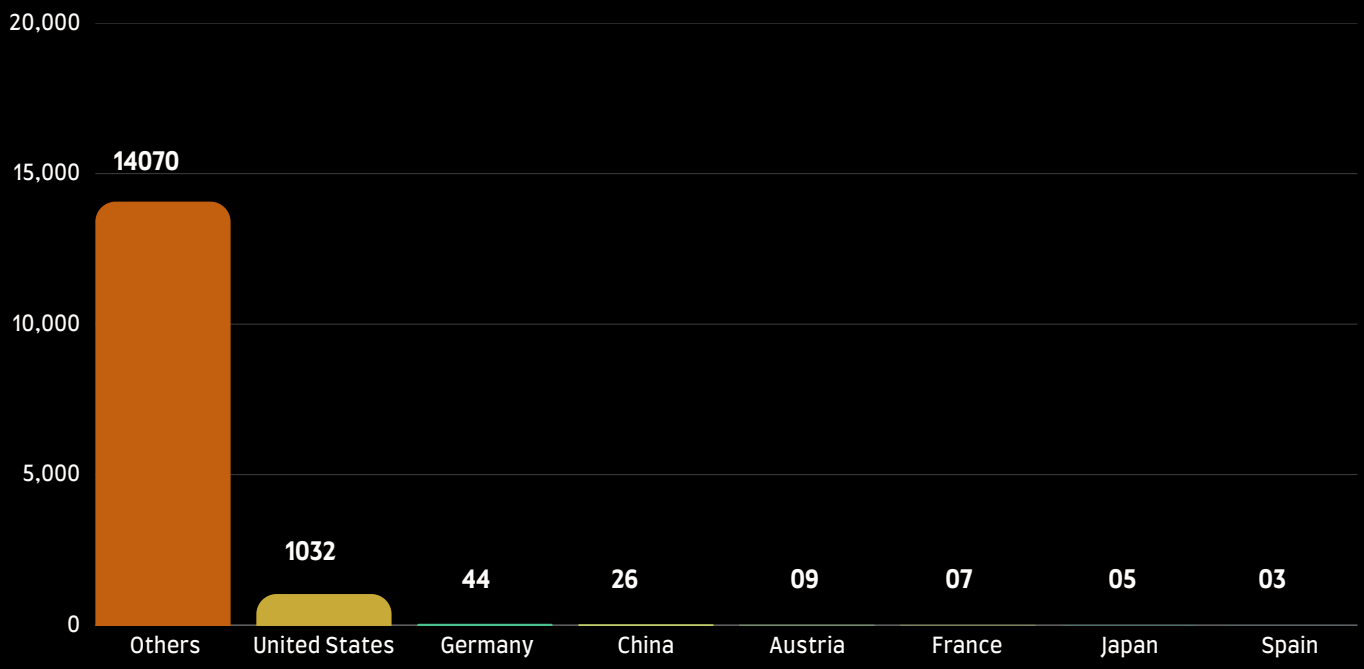
CVE ID	CVSS Score	Severity
CVE-2026-42369	10.0	Critical
CVE-2026-7411	10.0	Critical
CVE-2026-42826	10.0	Critical
CVE-2025-40805	10.0	Critical
CVE-2026-20182	10.0	Critical
CVE-2026-44523	10.0	Critical

KEY HIGHLIGHTS

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

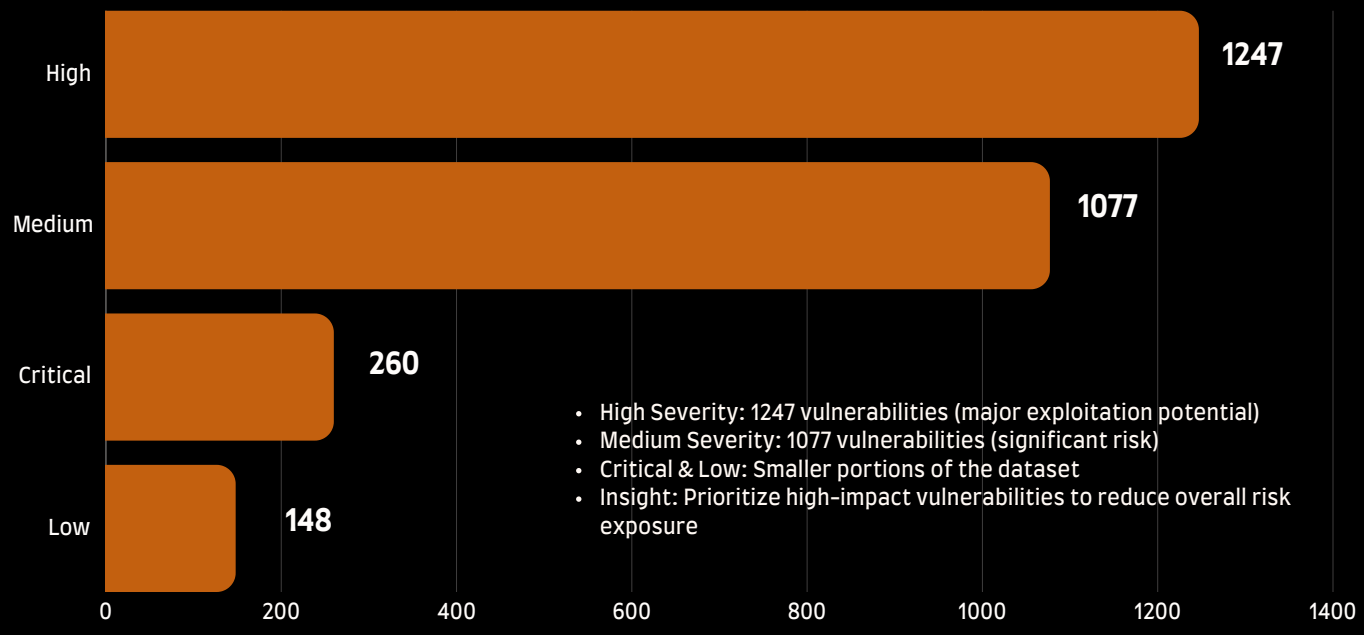
+91 7842046995 reach@castellumlabs.com www.castellumlabbs.com

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 (94.8%) have fixes available, but 5.2% remain unpatched, emphasizing the ongoing risk and the importance of timely patching.

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

CVE-2026-42369

Overview

A critical vulnerability has been identified in GV-VMS that can allow remote attackers to execute arbitrary code on Windows systems. The issue affects the WebCam Server component and can lead to full SYSTEM-level compromise.

Technical Details

The vulnerability occurs in the gvapi endpoint when a long base64-decoded authentication string is copied into a fixed 256-byte stack buffer without bounds checking. A crafted request can trigger a stack overflow, allowing attackers to execute arbitrary code as SYSTEM due to the lack of ASLR protection.

Vendor: GeoVision Inc.
Affected Product: GV-VMS V20.0.2
Affected Versions: V20.0.2

- **Published Date:** 04-05-2026
- **Last Patch:** 15-05-2026
- **Vulnerability Type:** Stack Overflow / Remote Code Execution
- **Fix Available:** Yes
- **Patched Version:** V20.0.2.10, V20.1.0.0

Exploitaion Status

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

Reference: https://www.geovision.com.tw/cyber_security.php
https://https://talosintelligence.com/vulnerability_reports/

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

CVE-2026-7411

Overview

A critical vulnerability has been identified in Eclipse BaSyx that allows unauthenticated attackers to perform path traversal through the Submodel HTTP API. Successful exploitation can lead to arbitrary file write and potentially remote code execution on the host system.

Technical Details

The vulnerability is caused by inadequate path normalization in the fileName parameter during file upload operations in the Submodel HTTP API. An attacker can supply crafted path traversal input to write files outside the intended directory, leading to possible code execution.

Vendor: Eclipse Foundation
Affected Product: Eclipse BaSyx
Affected Versions: 0 before 2.0.0-milestone-10

- **Published Date:** 05-05-2026
- **Last Patch:** 05-05-2026
- **Vulnerability Type:** Path Traversal / Arbitrary File Write / Remote Code Execution
- **Fix Available:** Yes
- **Patched Version:** 2.0.0-milestone-10

Exploitation Status

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

Reference: https://gitlab.eclipse.org/security/vulnerability-reports/-/issues/423
https://gitlab.eclipse.org/security/cve-assignment/-/issues/102

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

CVE-2026-42826

Overview

A critical vulnerability has been identified in Azure DevOps that may allow unauthorized attackers to access sensitive information over a network. The issue affects Microsoft's hosted Azure DevOps service and can result in exposure of confidential data to unauthorized users.

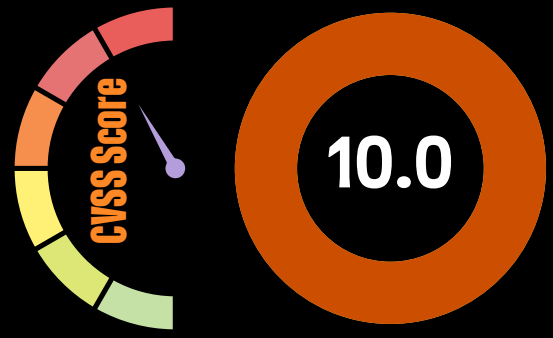
Technical Details

The vulnerability occurs due to improper access control, which may expose sensitive information to unauthorized actors. An attacker can exploit the issue remotely without authentication to retrieve confidential data from the affected service.

Microsoft

Affected Product: Azure DevOps
Affected Versions: Not Available
Vendor: Microsoft

- **Published Date:** 07-05-2026
- **Last Patch:** 15-05-2026
- **Vulnerability Type:** Information Disclosure / Sensitive Information Exposure
- **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://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42826

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

CVE-2025-40805

Overview

A critical vulnerability has been identified in Industrial Edge Cloud Device (IECD) that allows unauthenticated attackers to bypass authentication on specific API endpoints. Successful exploitation may let attackers impersonate legitimate users and gain unauthorized access to the affected device.

Technical Details

The vulnerability exists because certain API endpoints do not properly enforce user authentication before processing requests. An attacker who knows the identity of a valid user can exploit this flaw to bypass authorization checks and impersonate that user.

SIEMENS

Affected Product: Industrial Edge Cloud Device
Affected Versions: 0 before V1.24.2
Vendor: Siemens

- **Published Date:** 13-01-2026
- **Last Patch:** 12-05-2026
- **Vulnerability Type:** Authentication Bypass / Authorization Bypass
- **Fix Available:** Yes
- **Patched Version:** V1.24.2

Exploitation Status

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

Reference: https://cert-portal.siemens.com/productcert/html/ssa-014678.html
https://cert-portal.siemens.com/productcert/html/ssa-001536.html

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

CVE-2026-20182

Overview

A critical vulnerability has been identified in Cisco Catalyst SD-WAN Manager that allows unauthenticated remote attackers to bypass authentication. Successful exploitation may grant administrative-level access to the SD-WAN controller and allow manipulation of network configurations.

Technical Details

The vulnerability exists because the peering authentication mechanism in the control connection handshaking process does not function correctly. An attacker can send crafted requests to bypass authentication and log in as a high-privileged internal user, enabling access to NETCONF and network control.

Affected Product: **Cisco Catalyst SD-WAN Manager**
Affected Versions: **Multiple versions (including 17.2.x, 18.x, 19.2.x, 20.1.x, 20.3.2)**
Vendor: **Cisco**

- **Published Date:** 14-05-2026
- **Last Patch:** 14-05-2026
- **Vulnerability Type:** Improper Authentication / Authentication Bypass
- **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

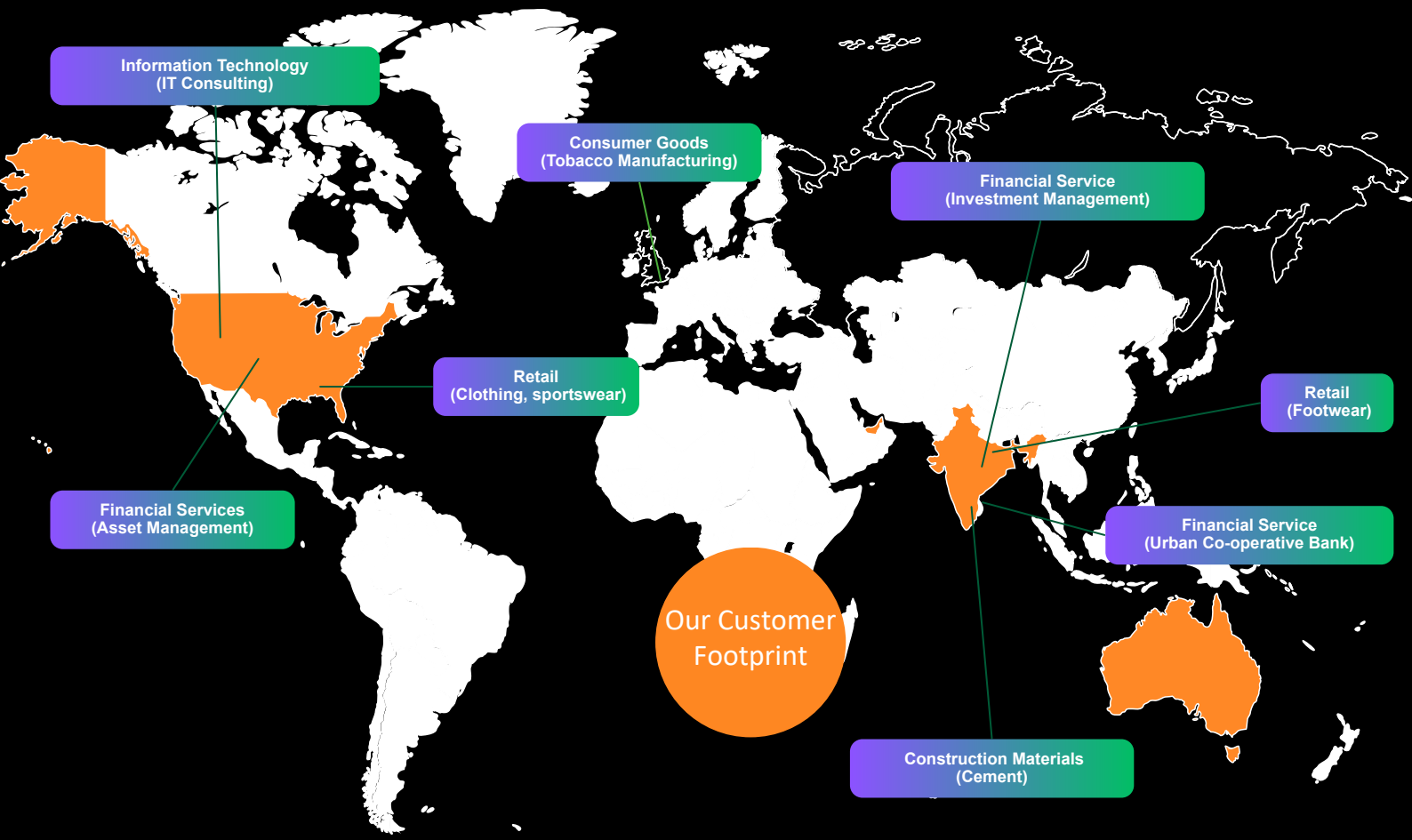
Reference:https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa2-v69WY2SW

+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