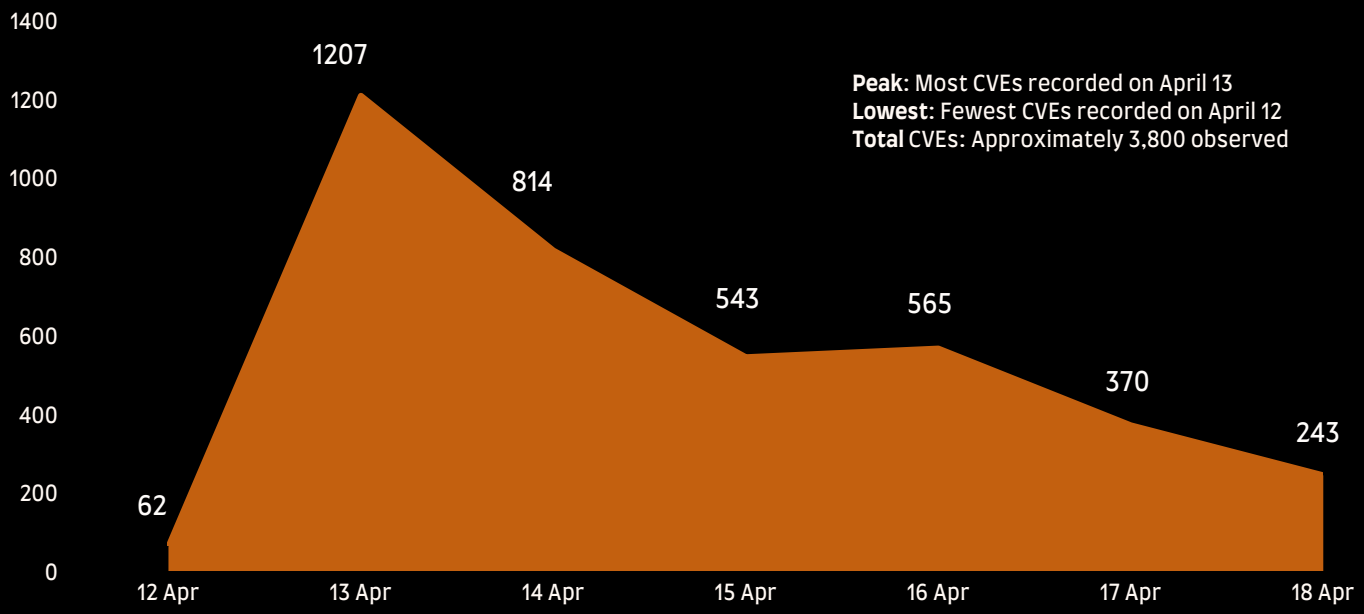
# CVE WEEKLY REPORT

## Number of CVE this week




## Top CVE this week

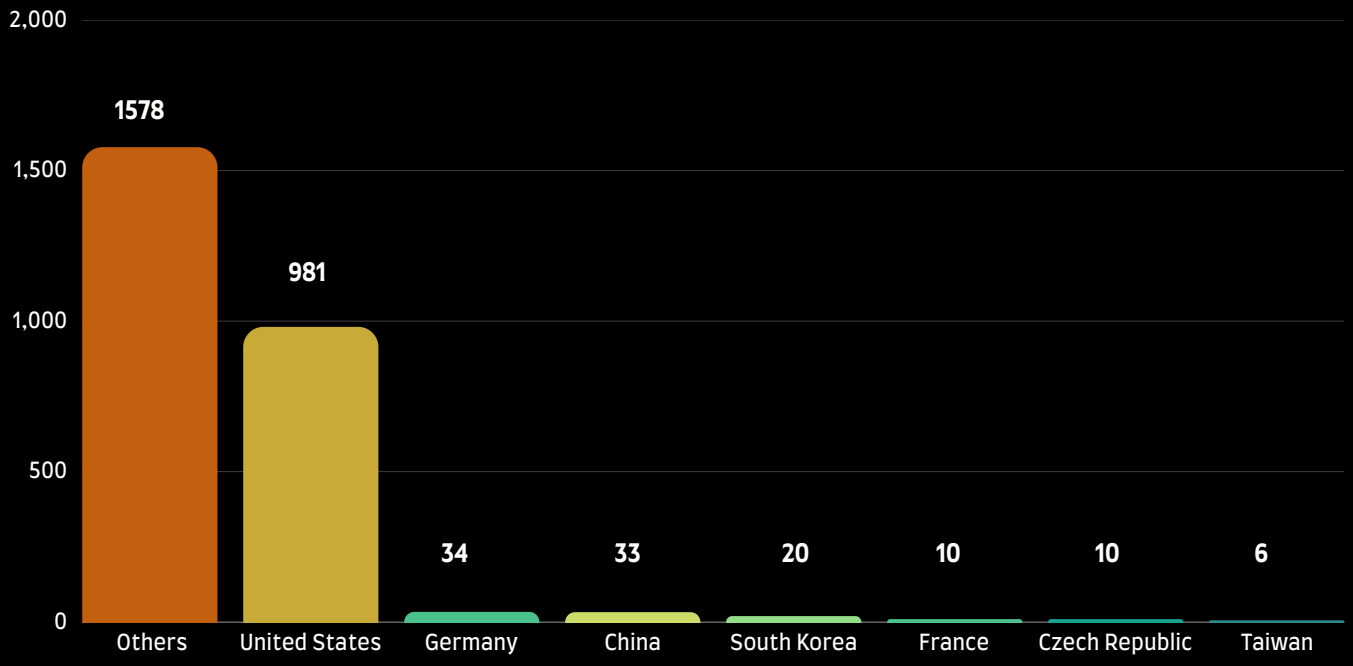
| CVE ID | CVSS Score | Severity |
|---|---|---|
| CVE-2026-4149 | 10.0 | Critical |
| CVE-2026-32169 | 10.0 | Critical |
| CVE-2026-35031 | 10.0 | Critical |
| CVE-2026-39842 | 10.0 | Critical |
| CVE-2025-41115 | 10.0 | Critical |
| CVE-2025-65037 | 10.0 | Critical |

## KEY HIGHLIGHTS

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

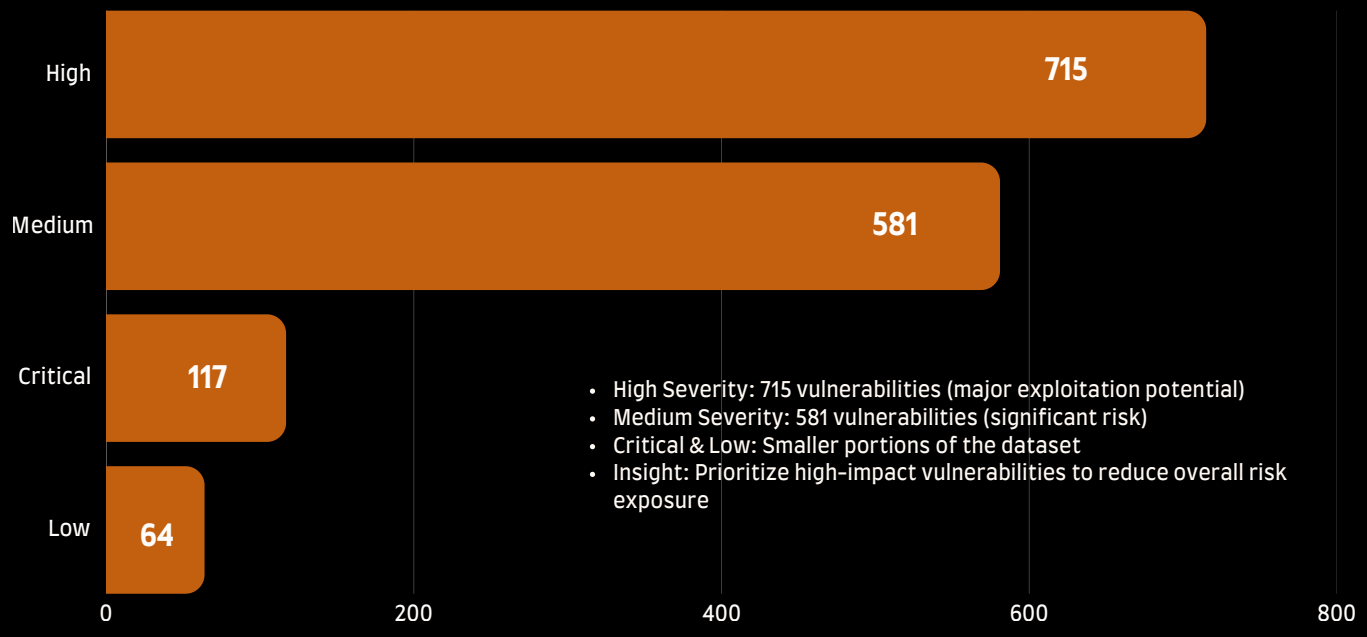
+91 7842046995 reach@castellumlabs.com www.castellumlabbs.com

## 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 (84.1%) have fixes available, but 15.9% remain unpatched, emphasizing the ongoing risk and the importance of timely patching.

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

# CVE-2026-4149

## Overview

A critical vulnerability has been identified in Sonos Era 300 speakers. The flaw allows remote attackers to execute arbitrary code by sending a specially crafted SMB response, potentially gaining kernel-level code execution without authentication

## Technical Details

A flaw in SMB DataOffset handling (CWE-119) allows remote attackers to execute kernel-level code without authentication via out-of-bounds memory access.

- **Affected Product:** Sonos Era 300
- **Affected Versions:**17.5 (build 91.0-70070)
- **Vendor:** Sonos
- **Published Date:** 11-04-2026
- **Last Patch:** 11-04-2026
- **Vulnerability Type:** Out-of-Bounds Memory Access / Remote Code Execution
- **Fix Available:** No
- **Patched Version:** Not Available



## Exploitaion Status

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

**Reference:** https://www.zerodayinitiative.com/advisories/ZDI-26-192/

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

# CVE-2026-32169

## Overview

A critical vulnerability has been identified in Azure Cloud Shell. The flaw is a Server-Side Request Forgery (SSRF) issue that could allow an unauthorized remote attacker to elevate privileges over a network.

## Technical Details

CWE-918 SSRF vulnerability in Azure Cloud Shell allows remote attackers to force internal requests and escalate privileges without user interaction or authentication.

- **Affected Product:** Azure Cloud Shell
- **Affected Versions:** Not Available
- **Vendor:** Microsoft
- **Published Date:** 19-03-2026
- **Last Patch:** 14-04-2026
- **Vulnerability Type:** SSRF / Privilege Escalation
- **Fix Available:** No
- **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-2026-32169

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

# CVE-2026-39842

## Overview

A critical vulnerability has been identified in Jellyfin Media Server. The flaw allows attackers with subtitle upload permissions to exploit path traversal and arbitrary file write issues, which can be chained into privilege escalation and remote code execution as root.

## Technical Details

A flaw in the subtitle upload endpoint (POST /Videos/{itemId}/Subtitles) allows path traversal via the Format field, enabling arbitrary file writes, reads, database access, privilege escalation, and root-level remote code execution.
This exploitation needs an administrator or a user with Upload Subtitles permission

- **Affected Product:** Jellyfin Media Server
- **Affected Versions:** All versions prior to 10.11.7
- **Vendor:** Jellyfin
- **Published Date:** 14-04-2026
- **Last Patch:** 23-04-2026
- **Vulnerability Type:** Path Traversal / Arbitrary File Write / Privilege Escalation /
- **Fix Available:** Yes
- **Patched Version:** 10.11.7 or later



## Exploitation Status

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

**Reference:** https://github.com/jellyfin/jellyfin/security/advisories/GHSA-j2hf-x4q5-47j3

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

# CVE-2026-39842

## Overview

A critical vulnerability has been identified in OpenRemote IoT Platform. The flaw allows authenticated attackers to execute arbitrary code on the server through expression injection vulnerabilities in the rules engine, potentially leading to full system compromise

## Technical Details

The vulnerability stems from two interrelated issues in the rules engine:

1. JavaScript rules use Nashorn ScriptEngine.eval() without sandboxing or access restrictions.
2. Groovy security filters were defined but never properly registered.

- **Affected Product:** OpenRemote
- **Affected Versions:** 1.21.0 and below
- **Vendor:** OpenRemote
- **Published Date:** 2026-04-14
- **Last Patch:** 2026-04-14
- **Vulnerability Type:** Expression Injection / Remote Code Execution
- **Fix Available:** Yes
- **Patched Version:** 1.22.0



## Exploitation Status

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

**Reference:**https://github.com/openremote/openremote/security/advisories/GHSA-7mqr-33rv-p3mp

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

# CVE-2025-41115

## Overview

A critical vulnerability has been identified in Grafana Enterprise and Grafana Cloud. The flaw allows a malicious or compromised SCIM client to impersonate users or gain elevated privileges through improper identity handling during SCIM provisioning

## Technical Details

When SCIM provisioning is enabled, a malicious client sending a numeric externalId can override internal user IDs.
This will potentially lead to user impersonation or privilege escalation.

- **Affected Product:** Grafana Enterprise / Grafana Cloud
- **Affected Versions:** 12.0.0 to before 12.2.1
- **Vendor:** Grafana Labs
- **Published Date:** 2025-11-21
- **Last Patch:** 2026-04-24
- **Vulnerability Type:** Privilege Escalation / User Impersonation / Incorrect Privilege Assignment
- **Fix Available:** Yes
- **Patched Version:** 12.2.1



## Exploitation Status

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

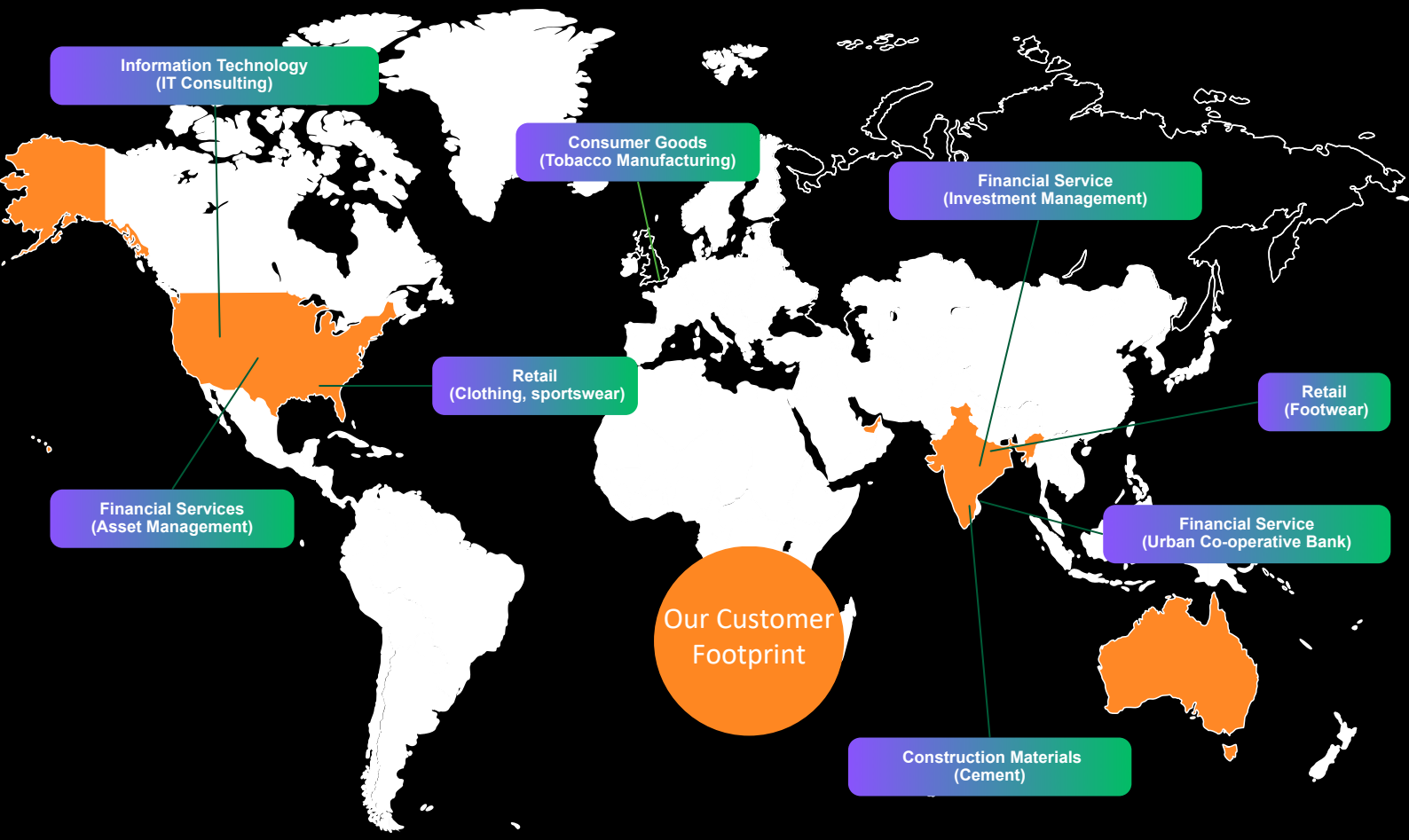
**Reference:** https://grafana.com/security/security-advisories/cve-2025-41115

+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**