# Cybersecurity Intelligence Report

**Generated:** 2025-10-23 04:37:02 **Analysis Period:** Last 10 days **Report Classification:** CONFIDENTIAL

## Executive Summary

This report provides a comprehensive analysis of the current cybersecurity threat landscape. The primary focus is a direct "Threat-to-Action" model, outlining immediate responses to active threats.

### Threat Level Assessment

**Current Threat Level: CRITICAL** - Immediate action required

## 1. Active Threat Analysis & Response

This section links active threats directly to their recommended mitigation strategies.

### 1.1 Threat: Critical Vulnerability Exploit: CVE-2025-11661

**Severity:** HIGH
**Date:** 2025-10-13T05:15:49.833
**Source:** NVD
**Description:** A vulnerability was found in ProjectsAndPrograms School Management System up to 6b6fae5426044f89c08d0dd101c7fa71f9042a59. This affects an unknown part. Performing manipulation results in missing authe...

* *RECOMMENDED ACTION:**

**Priority:** CRITICAL **Recommendations:** - Apply vendor-supplied patches or workarounds immediately - Restrict network access to vulnerable systems

**Implementation Steps:** - Identify all affected systems using vulnerability scanner - Apply virtual patching if official patch is unavailable - Hunt for IOCs related to CVE-2025-11661

### 1.2 Threat: Critical Vulnerability Exploit: CVE-2025-11662

**Severity:** HIGH
**Date:** 2025-10-13T05:15:50.763
**Source:** NVD
**Description:** A security flaw has been discovered in SourceCodester Best Salon Management System 1.0. Impacted is an unknown function of the file /booking.php. The manipulation of the argument serv_id results in sq...

* *RECOMMENDED ACTION:**

**Priority:** CRITICAL **Recommendations:** - Apply vendor-supplied patches or workarounds immediately - Restrict network access to vulnerable systems

**Implementation Steps:** - Identify all affected systems using vulnerability scanner - Apply virtual patching if official patch is unavailable - Hunt for IOCs related to CVE-2025-11662

### 1.3 Threat: Critical Vulnerability Exploit: CVE-2025-11664

**Severity:** MEDIUM
**Date:** 2025-10-13T07:15:50.563
**Source:** NVD
**Description:** A security vulnerability has been detected in Campcodes Online Beauty Parlor Management System 1.0. The impacted element is an unknown function of the file /admin/search-appointment.php. Such manipula...

* *RECOMMENDED ACTION:**

**Priority:** CRITICAL **Recommendations:** - Apply vendor-supplied patches or workarounds immediately - Restrict network access to vulnerable systems

**Implementation Steps:** - Identify all affected systems using vulnerability scanner - Apply virtual patching if official patch is unavailable - Hunt for IOCs related to CVE-2025-11664

## 1.4 Threat: Critical Vulnerability Exploit: CVE-2025-27258

**Severity:** CRITICAL
**Date:** 2025-10-13T07:15:54.227
**Source:** NVD
**Description:** Ericsson Network Manager (ENM) versions prior to ENM 25.1 GA contain a vulnerability, if exploited, can result in an escalation of privilege....

* *RECOMMENDED ACTION:**

**Priority:** CRITICAL **Recommendations:** - Apply vendor-supplied patches or workarounds immediately - Restrict network access to vulnerable systems

**Implementation Steps:** - Identify all affected systems using vulnerability scanner - Apply virtual patching if official patch is unavailable - Hunt for IOCs related to CVE-2025-27258

---

## 1.5 Threat: Critical Vulnerability Exploit: CVE-2025-42910

**Severity:** CRITICAL
**Date:** 2025-10-14T01:15:32.880
**Source:** NVD
**Description:** Due to missing verification of file type or content, SAP Supplier Relationship Management allows an authenticated attacker to upload arbitrary files. These files could include executables which might ...

* *RECOMMENDED ACTION:**

**Priority:** CRITICAL **Recommendations:** - Apply vendor-supplied patches or workarounds immediately - Restrict network access to vulnerable systems

**Implementation Steps:** - Identify all affected systems using vulnerability scanner - Apply virtual patching if official patch is unavailable - Hunt for IOCs related to CVE-2025-42910

---

## 1.6 Threat: Ransomware Campaign Targeting Healthcare Sector

**Severity:** CRITICAL
**Date:** 2025-10-22
**Source:** Simulated Threat Intel
**Description:** New ransomware variant 'BlackCat 2.0' actively targeting healthcare organizations with double extortion tactics

* *RECOMMENDED ACTION:**

**Priority:** CRITICAL **Recommendations:** - Implement robust backup and recovery procedures (3-2-1 rule) - Deploy endpoint detection and response (EDR) solutions

**Implementation Steps:** - Verify all critical data backups are offline and immutable - Configure EDR to block common ransomware behaviors

---

## 1.7 Threat: Phishing Campaign Using Fake Microsoft 365 Login Pages

**Severity:** HIGH
**Date:** 2025-10-21
**Source:** Simulated Threat Intel
**Description:** Widespread phishing campaign detected using lookalike Microsoft 365 domains to harvest credentials

* *RECOMMENDED ACTION:**

**Priority:** HIGH **Recommendations:** - Deploy multi-factor authentication (MFA) across all external systems - Implement email authentication (SPF, DKIM, DMARC)

**Implementation Steps:** - Enforce MFA for all user accounts immediately - Configure DMARC policy to reject or quarantine

---

# 2. Vulnerability Analysis & Response

This section lists high-impact vulnerabilities and their grouped mitigation plans.

## 2.2 High Vulnerability Response (HIGH)

**Recommendations:** - Address all 8 identified HIGH vulnerabilities within 14 days - Follow standard patch management procedures

**Implementation Steps:** - Schedule patches in the next available maintenance window - Verify remediation with a follow-up vulnerability scan

### Detailed Vulnerability List:

**1. CVE-2025-11667** (CVSS: 6.3 - MEDIUM ) - **Description:** A vulnerability was found in code-projects Automated Voting System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/... - **Products:** `fabian:automated_voting_system`

**2. CVE-2025-11668** (CVSS: 4.7 - MEDIUM ) - **Description:** A vulnerability was determined in code-projects Automated Voting System 1.0. Affected by this issue is some unknown functionality of the file /admin/u... - **Products:** `fabian:automated_voting_system`

**3. CVE-2025-11673** (CVSS: 7.2 - HIGH ) - **Description:** SOOP-CLM developed by PiExtract has a Hidden Functionality vulnerability, allowing privileged remote attackers to exploit a hidden functionality to ex...

**4. CVE-2025-11675** (CVSS: 7.2 - HIGH ) - **Description:** Enterprise Cloud Database developed by Ragic has an Arbitrary File Upload vulnerability, allowing privileged remote attackers to upload and execute we...

**5. CVE-2025-9902** (CVSS: 7.5 - HIGH ) - **Description:** Authorization Bypass Through User-Controlled Key vulnerability in AKIN Software Computer Import Export Industry and Trade Co. Ltd. QRMenu allows Privi...

**6. CVE-2025-7707** (CVSS: 7.8 - HIGH ) - **Description:** The llama_index library version 0.12.33 sets the NLTK data directory to a subdirectory of the codebase by default, which is world-writable in multi-us... - **Products:** `llamaindex:llamaindex`

**7. CVE-2025-62177** (CVSS: 8.8 - HIGH ) - **Description:** WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. Prior to 3.5.1, a SQL Injection vulnerability was iden... - **Products:** `wegia:wegia`

**8. CVE-2025-62179** (CVSS: 8.8 - HIGH ) - **Description:** WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. Prior to 3.5.1, a SQL Injection vulnerability was iden... - **Products:** `wegia:wegia`

**9. CVE-2025-62360** (CVSS: 8.8 - HIGH ) - **Description:** WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users.Prior to 3.5.1, a SQL Injection vulnerability was ident... - **Products:** `wegia:wegia`

**10. CVE-2025-41703** (CVSS: 7.5 - HIGH ) - **Description:** An unauthenticated remote attacker can cause a Denial of Service by turning off the output of the UPS via Modbus command....

## 3. General Security Posture Recommendations

**Priority:** MEDIUM **Recommendations:** - Conduct regular security assessments and penetration testing - Maintain a comprehensive asset inventory - Enforce the principle of least privilege

**Implementation Steps:** - Schedule quarterly internal/external vulnerability scans - Deploy a CMDB or asset management solution - Review and revoke unnecessary user permissions monthly

## 4. Security Metrics

| Metric | Value |
|---|---|
| **Total Threats Identified** | **7** |
| **Critical Threats** | **3** |
| **Total Vulnerabilities** | **10** |
| **Critical CVEs** | **0** |

## 5. Report Generation Details

**System:** Cybersecurity Intelligence Platform v1.0
**Analysis Engine:** Rule-Based System (Multi-Agent AI Disabled)
**Data Sources:** NVD, Simulated Feeds