Posted Date: 2025/11/05

[Vulnerability Alert] CISA Added 8 Known Exploited Vulnerabilities to KEV Catalog (2025/10/20-2025/10/26)

- Subject: [Vulnerability Alert] CISA Added 8 Known Exploited Vulnerabilities to KEV Catalog (2025/10/20-2025/10/26)
- Content:
  - Forwarded from Taiwan Computer Emergency Response Team/Coordination Center TWCERTCC-200-202510-00000014

1. [CVE-2022-48503] Apple Multiple Products Unspecified Vulnerability (CVSS v3.1: 8.8)
   - [Exploited by Ransomware: Unknown] An unspecified vulnerability exists in JavaScriptCore in Apple macOS, iOS, tvOS, Safari, and watchOS which may lead to arbitrary code execution when processing web content. The affected products may have reached End-of-Life (EoL) or End-of-Service (EoS), and users are advised to stop using the product.
   - [Affected Platforms] Please refer to the official listed affected versions
   - https://support.apple.com/en-us/102879
   - https://support.apple.com/en-us/102893
   - https://support.apple.com/en-us/102878
   - https://support.apple.com/en-us/102891
   - https://support.apple.com/en-us/102892
2. [CVE-2025-2746] Kentico Xperience CMS Authentication Bypass Using an Alternate Path or Channel Vulnerability (CVSS v3.1: 9.8)
   - [Exploited by Ransomware: Unknown] Kentico Xperience CMS has an authentication bypass vulnerability using an alternate path or channel. The Staging Sync Server improperly handles a blank SHA1 username during digest authentication, which may allow an attacker to gain control over administrative objects.
   - [Affected Platforms] Kentico Xperience versions prior to 130.172
3. [CVE-2025-2747] Kentico Xperience CMS Authentication Bypass Using an Alternate Path or Channel Vulnerability (CVSS v3.1: 9.8)
   - [Exploited by Ransomware: Unknown] Kentico Xperience CMS has an authentication bypass vulnerability using an alternate path or channel. The Staging Sync Server component has a weak password handling when the server is configured to “None” type, which may allow an attacker to gain control over administrative objects.
   - [Affected Platforms] Kentico Xperience versions prior to 130.178
4. [CVE-2025-33073] Microsoft Windows SMB Client Improper Access Control Vulnerability (CVSS v3.1: 8.8)
   - [Exploited by Ransomware: Unknown] Microsoft Windows SMB Client has an improper access control vulnerability. An attacker can induce the victim to actively establish and authenticate an SMB connection to the attacker's SMB server, which may allow the attacker to elevate privileges on the victim system or perform unauthorized operations.
   - [Affected Platforms] Please refer to the official listed affected versions
   - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-33073
5. [CVE-2025-61884] Oracle E-Business Suite Server-Side Request Forgery (SSRF)

Vulnerability (CVSS v3.1: 7.5)
    - [Exploited by Ransomware: Known] Oracle E-Business Suite has a Server-Side Request Forgery vulnerability in the Runtime component of Oracle Configurator. This vulnerability can be exploited remotely and without authentication.
    - [Affected Platforms] Please refer to the official listed affected versions
    - https://www.oracle.com/security-alerts/alert-cve-2025-61884.html
6. [CVE-2025-61932] Motex LANSCOPE Endpoint Manager Improper Verification of Source of a Communication Channel Vulnerability (CVSS v3.1: 9.8)
    - [Exploited by Ransomware: Unknown] Motex LANSCOPE Endpoint Manager has an improper verification of source of a communication channel vulnerability. An attacker can execute arbitrary code by sending specially crafted packets.
    - [Affected Platforms] Please refer to the official listed affected versions
    - https://www.motex.co.jp/news/notice/2025/release251020/
7. [CVE-2025-54236] Adobe Commerce and Magento Improper Input Validation Vulnerability (CVSS v3.1: 9.1)
    - [Exploited by Ransomware: Unknown] Adobe Commerce and Magento Open Source have an improper input validation vulnerability. An attacker may be able to take over customer accounts via the Commerce REST API.
    - [Affected Platforms] Please refer to the official listed affected versions
    - https://helpx.adobe.com/security/products/magento/apsb25-88.html
8. [CVE-2025-59287] Microsoft Windows Server Update Service (WSUS) Deserialization of Untrusted Data Vulnerability (CVSS v3.1: 9.8)
    - [Exploited by Ransomware: Unknown] Microsoft Windows Server Update Service (WSUS) has a deserialization of untrusted data vulnerability, which may lead to remote code execution.
    - [Affected Platforms] Please refer to the official listed affected versions
    - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-59287

- Affected Platforms:
    - Detailed content in the Affected Platforms section of Content Description
- Recommended Measures:
    1. [CVE-2022-48503] The official source has released a fix update for the vulnerability; please update to the relevant version
        - https://support.apple.com/en-us/102879
        - https://support.apple.com/en-us/102893
        - https://support.apple.com/en-us/102878
        - https://support.apple.com/en-us/102891
        - https://support.apple.com/en-us/102892
    2. [CVE-2025-2746] The official source has released a fix update for the vulnerability; please update to the relevant version
        - https://devnet.kentico.com/download/hotfixes
    3. [CVE-2025-2747] The official source has released a fix update for the vulnerability; please update to the relevant version
        - https://devnet.kentico.com/download/hotfixes
    4. [CVE-2025-33073] The official source has released a fix update for the vulnerability; please update to the relevant version
        - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-33073
    5. [CVE-2025-61884] The official source has released a fix update for the vulnerability; please update to the relevant version
        - https://www.oracle.com/security-alerts/alert-cve-2025-61884.html
    6. [CVE-2025-61932] The official source has released a fix update for the vulnerability;

please update to the relevant version
   - https://www.motex.co.jp/news/notice/2025/release251020/
7. [CVE-2025-54236] The official source has released a fix update for the vulnerability; please update to the relevant version
   - https://helpx.adobe.com/security/products/magento/apsb25-88.html
8. [CVE-2025-59287] The official source has released a fix update for the vulnerability; please update to the relevant version
   - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-59287

Computer and Communications Center
Network Systems Group