Posted Date: 2025/05/30

【Vulnerability Alert】 CISA Adds 7 Newly Exploited Vulnerabilities to the KEV Catalog (2025/05/19–2025/05/25)

- Subject Description: 【Vulnerability Alert】 CISA Adds 7 Newly Exploited Vulnerabilities to the KEV Catalog (2025/05/19–2025/05/25)

- Content Description:
  - Forwarded from Taiwan Computer Emergency Response Team/Coordination Center TWCERTCC-200-202505-00000022

1. [CVE-2023-38950] ZKTeco BioTime Path Traversal Vulnerability (CVSS v3.1: 7.5)
   - [Ransomware Exploitation: Unknown] A path traversal vulnerability exists in the iclock API of ZKTeco BioTime, allowing unauthenticated attackers to read arbitrary files by providing specially crafted payloads.
   - [Affected Platforms] Refer to the affected versions listed by the vendor
   - https://www.zkteco.com/en/Security_Bulletinsibs/10
2. [CVE-2024-27443] Synacor Zimbra Collaboration Suite (ZCS) Cross-Site Scripting (XSS) Vulnerability (CVSS v3.1: 6.1)
   - [Ransomware Exploitation: Unknown] A cross-site scripting vulnerability exists in the CalendarInvite feature of the Zimbra Webmail Classic UI, which can be exploited via specially crafted email messages containing malicious calendar headers to execute arbitrary JavaScript.
   - [Affected Platforms] Refer to the affected versions listed by the vendor
   - https://wiki.zimbra.com/wiki/Zimbra_Releases/10.0.7#Security_Fixes
   - https://wiki.zimbra.com/wiki/Zimbra_Releases/9.0.0/P39#Security_Fixes
3. [CVE-2025-27920] Srimax Output Messenger Directory Traversal Vulnerability (CVSS v3.1: 6.5)
   - [Ransomware Exploitation: Unknown] A directory traversal vulnerability in Srimax Output Messenger allows attackers to access sensitive files outside the intended directory, potentially exposing configurations or enabling arbitrary file access.
   - [Affected Platforms] Refer to the affected versions listed by the vendor
   - https://www.outputmessenger.com/cve-2025-27920/
4. [CVE-2024-11182] MDaemon Email Server Cross-Site Scripting (XSS) Vulnerability (CVSS v3.1: 6.1)
   - [Ransomware Exploitation: Unknown] A cross-site scripting vulnerability exists in the MDaemon Email Server, allowing remote attackers to load arbitrary JavaScript via HTML emails.
   - [Affected Platforms] Refer to the affected versions listed by the vendor
   - https://mdaemon.com/pages/downloads-critical-updates
5. [CVE-2025-4428] Ivanti Endpoint Manager Mobile (EPMM) Code Injection Vulnerability (CVSS v3.1: 8.8)
   - [Ransomware Exploitation: Unknown] A code injection vulnerability exists in the API component of Ivanti EPMM, allowing authenticated attackers to execute arbitrary code remotely via crafted API requests. This vulnerability stems from insecure

implementation of the Hibernate Validator open-source library.
    - [Affected Platforms] Refer to the affected versions listed by the vendor
    - https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM?language=en_US
6. [CVE-2025-4427] Ivanti Endpoint Manager Mobile (EPMM) Authentication Bypass Vulnerability (CVSS v3.1: 7.5)
    - [Ransomware Exploitation: Unknown] An authentication bypass vulnerability in the API component of Ivanti EPMM allows attackers to access protected resources without proper credentials using specially crafted API requests. This stems from insecure implementation of the Spring Framework open-source library.
    - [Affected Platforms] Refer to the affected versions listed by the vendor
    - https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM?language=en_US
7. [CVE-2025-4632] Samsung MagicINFO 9 Server Path Traversal Vulnerability (CVSS v3.1: 9.8)
    - [Ransomware Exploitation: Unknown] A path traversal vulnerability in Samsung MagicINFO 9 Server allows attackers to write arbitrary files with system privileges.
    - [Affected Platforms] Refer to the affected versions listed by the vendor
    - https://security.samsungtv.com/securityUpdates#SVP-MAY-2025

- Affected Platforms:
    - For details, refer to the affected platforms listed in the content description
- Recommended Actions:
    1. [CVE-2023-38950] Official fixes have been released; please update to the appropriate version
        - https://www.zkteco.com/en/Security_Bulletinsibs/10
    2. [CVE-2024-27443] Official fixes have been released; please update to the appropriate version
        - https://wiki.zimbra.com/wiki/Zimbra_Releases/10.0.7#Security_Fixes
        - https://wiki.zimbra.com/wiki/Zimbra_Releases/9.0.0/P39#Security_Fixes
    3. [CVE-2025-27920] Official fixes have been released; please update to the appropriate version
        - https://www.outputmessenger.com/cve-2025-27920/
    4. [CVE-2024-11182] Official fixes have been released; please update to the appropriate version
        - https://mdaemon.com/pages/downloads-critical-updates
    5. [CVE-2025-4428] Official fixes have been released; please update to the appropriate version
        - https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM?language=en_US
    6. [CVE-2025-4427] Official fixes have been released; please update to the appropriate version
        - https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM?language=en_US
    7. [CVE-2025-4632] Official fixes have been released; please update to the appropriate version
        - https://security.samsungtv.com/securityUpdates#SVP-MAY-2025

Computer and Communication Center

Network Systems Division

From:
https://net.nthu.edu.tw/netsys/ - **網路系統組**

Permanent link:
https://net.nthu.edu.tw/netsys/en:mailing:announcement:20250530_02

Last update: **2025/05/30 16:10**