Post Date: 2026/04/28

【Vulnerability Alert】CISA Adds 9 Known Exploited Vulnerabilities to KEV Catalog (2026/04/06-2026/04/12)

- Subject: 【Vulnerability Alert】CISA Adds 9 Known Exploited Vulnerabilities to KEV Catalog (2026/04/06-2026/04/12)

- Description:
  - Forwarded from Taiwan Computer Emergency Response Team / Coordination Center Security Alert TWCERTCC-200-202604-00000013
  - 【CVE-2026-35616】Fortinet FortiClient EMS Improper Access Control Vulnerability (CVSS v3.1: 9.8)
  - 【Ransomware Exploitation: Unknown】 An improper access control vulnerability exists in Fortinet FortiClient EMS, which may allow an unauthenticated attacker to execute unauthorized code or commands via specially crafted requests.
  - 【CVE-2026-1340】Ivanti Endpoint Manager Mobile (EPMM) Code Injection Vulnerability (CVSS v3.1: 9.8)
  - 【Ransomware Exploitation: Unknown】 A code injection vulnerability exists in Ivanti Endpoint Manager Mobile (EPMM), which may allow an attacker to achieve remote code execution without authentication.
  - 【CVE-2012-1854】Microsoft Visual Basic for Applications Insecure Library Loading Vulnerability (CVSS v3.1: 7.8)
  - 【Ransomware Exploitation: Unknown】 An insecure library loading vulnerability exists in Microsoft Visual Basic for Applications (VBA), which may allow remote code execution.
  - 【CVE-2025-60710】Microsoft Windows Link Following Vulnerability (CVSS v3.1: 7.8)
  - 【Ransomware Exploitation: Unknown】 A link following vulnerability exists in Microsoft Windows, which may lead to privilege escalation.
  - 【CVE-2023-21529】Microsoft Exchange Server Deserialization of Untrusted Data Vulnerability (CVSS v3.1: 8.8)
  - 【Ransomware Exploitation: Unknown】 A deserialization of untrusted data vulnerability exists in Microsoft Exchange Server, which may allow an authenticated attacker to execute remote code.
  - 【CVE-2023-36424】Microsoft Windows Out-of-Bounds Read Vulnerability (CVSS v3.1: 7.8)
  - 【Ransomware Exploitation: Unknown】 An out-of-bounds read vulnerability exists in the Microsoft Windows Common Log File System driver, which may allow threat actors to perform privilege escalation.
  - 【CVE-2020-9715】Adobe Acrobat Use-After-Free Vulnerability (CVSS v3.1: 7.8)
  - 【Ransomware Exploitation: Unknown】 A use-after-free vulnerability exists in Adobe Acrobat, which may allow code execution.
  - 【CVE-2026-21643】Fortinet SQL Injection Vulnerability (CVSS v3.1: 9.8)
  - 【Ransomware Exploitation: Unknown】 An SQL injection vulnerability exists in Fortinet FortiClient EMS, which may allow an unauthenticated attacker to execute unauthorized code or commands via specially crafted HTTP requests.
  - 【CVE-2026-34621】Adobe Acrobat and Reader Prototype Pollution Vulnerability (CVSS

v3.1: 8.6)
    - □Ransomware Exploitation: Unknown□ A prototype pollution vulnerability exists in Adobe Acrobat and Reader, which may allow arbitrary code execution.
- Affected Platforms:
    - □CVE-2026-35616□Please refer to the official list of affected versions: https://fortiguard.fortinet.com/psirt/FG-IR-26-099
    - □CVE-2026-1340□Please refer to the official list of affected versions: https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-CVE-2026-1281-CVE-2026-1340
    - □CVE-2012-1854□Please refer to the official list of affected versions: https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2012/ms12-046
    - □CVE-2025-60710□Please refer to the official list of affected versions: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-60710
    - □CVE-2023-21529□Please refer to the official list of affected versions: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21529
    - □CVE-2023-36424□Please refer to the official list of affected versions: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36424
    - □CVE-2020-9715□Please refer to the official list of affected versions: https://helpx.adobe.com/security/products/acrobat/apsb20-48.html
    - □CVE-2026-21643□Please refer to the official list of affected versions: https://fortiguard.fortinet.com/psirt/FG-IR-25-1142
    - □CVE-2026-34621□Please refer to the official list of affected versions: https://helpx.adobe.com/security/products/acrobat/apsb26-43.html
- Recommended Actions:
    - □CVE-2026-35616□ The vendor has released a security update. Please update to the relevant version: https://fortiguard.fortinet.com/psirt/FG-IR-26-099
    - □CVE-2026-1340□ The vendor has released a security update. Please update to the relevant version: https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-CVE-2026-1281-CVE-2026-1340
    - □CVE-2012-1854□ The vendor has released a security update. Please update to the relevant version: https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2012/ms12-046
    - □CVE-2025-60710□ The vendor has released a security update. Please update to the relevant version: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-60710
    - □CVE-2023-21529□ The vendor has released a security update. Please update to the relevant version: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21529
    - □CVE-2023-36424□ The vendor has released a security update. Please update to the relevant version: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36424
    - □CVE-2020-9715□ The vendor has released a security update. Please update to the relevant version: https://helpx.adobe.com/security/products/acrobat/apsb20-48.html
    - □CVE-2026-21643□ The vendor has released a security update. Please update to the relevant version: https://fortiguard.fortinet.com/psirt/FG-IR-25-1142
    - □CVE-2026-34621□ The vendor has released a security update. Please update to the relevant version: https://helpx.adobe.com/security/products/acrobat/apsb26-43.html

---

Computer and Communication Center
Network Systems Division