Date Posted: 2025/10/22

[Vulnerability Alert] CISA Adds 6 Known Exploited Vulnerabilities to KEV Catalog (2025/10/13-2025/10/19)

- Subject: [Vulnerability Alert] CISA Adds 6 Known Exploited Vulnerabilities to KEV Catalog (2025/10/13-2025/10/19)
- Content:
    - Forwarded from Taiwan Computer Network Emergency Response Team/Coordination Center TWCERTCC-200-202510-00000011

    1. [CVE-2025-47827] IGEL OS Use of a Key Past its Expiration Date Vulnerability (CVSS v3.1: 4.6)
        - [Exploited by Ransomware: Unknown] IGEL OS has a security feature bypass vulnerability because the igel-flash-driver module does not correctly validate cryptographic signatures, allowing an attacker to bypass the secure boot mechanism and mount a specially crafted root file system from an unverified SquashFS image.
        - [Affected Platforms] Please refer to the affected versions listed by the vendor
        - https://kb.igel.com/en/security-safety/current/isn-2025-22-statement-on-cve-2025-47827-in-igel-os
    2. [CVE-2025-24990] Microsoft Windows Untrusted Pointer Dereference Vulnerability (CVSS v3.1: 7.8)
        - [Exploited by Ransomware: Unknown] Microsoft Windows Kernel-level Untrusted Pointer Dereference vulnerability, which may lead to local privilege escalation.
        - [Affected Platforms] Please refer to the affected versions listed by the vendor
        - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24990
    3. [CVE-2025-6264] Velociraptor API Improper Access Control Vulnerability (CVSS v3.1: 9.8)
        - [Exploited by Ransomware: Unknown] Velociraptor API has an Improper Access Control vulnerability, allowing an unauthenticated remote attacker to access the API port via HTTP and execute arbitrary code as an administrator.
        - [Affected Platforms] Please refer to the affected versions listed by the vendor
        - https://docs.velociraptor.app/announcements/advisories/cve-2025-6264/
    4. [CVE-2016-7836] SKYSEA Client View Improper Authentication Vulnerability (CVSS v3.1: 9.8)
        - [Exploited by Ransomware: Unknown] SKYSEA Client View has an Improper Authentication vulnerability. An attacker can achieve remote code execution through an authentication processing flaw during a TCP connection with the Management Console program.
        - [Affected Platforms] Please refer to the affected versions listed by the vendor
        - https://www.skygroup.jp/security-info/news/170308.html
    5. [CVE-2025-54253] Adobe Experience Manager Forms Code Execution Vulnerability (CVSS v3.1: 10.0)
        - [Exploited by Ransomware: Unknown] Adobe Experience Manager Forms in JEE has an unspecified vulnerability that may lead to arbitrary code execution.
        - [Affected Platforms] Please refer to the affected versions listed by the vendor
        - https://helpx.adobe.com/security/products/aem-forms/apsb25-82.html

    6. [CVE-2025-42937] SAP Print Service Directory Traversal Vulnerability (CVSS v3.1: 9.8)
        - [Exploited by Ransomware: Unknown] SAP Print Service has a Directory Traversal vulnerability, allowing an unauthenticated attacker to traverse directories and overwrite system files.
        - [Affected Platforms] Please refer to the affected versions listed by the vendor
        - https://support.sap.com/en/my-support/knowledge-base/security-notes-news/october-2025.html
- Affected Platforms:
    - Detailed content in the content description section's affected platforms
- Recommended Action:
    1. [CVE-2025-47827] The official vendor has released a statement on the vulnerability; please update to other unaffected versions
        - https://kb.igel.com/en/security-safety/current/isn-2025-22-statement-on-cve-2025-47827-in-igel-os
    2. [CVE-2025-24990] Please apply the official security update released by the vendor
        - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24990
    3. [CVE-2025-6264] Please refer to the official instructions for updating:
        - https://docs.velociraptor.app/announcements/advisories/cve-2025-6264/
    4. [CVE-2016-7836] Please refer to the official instructions for updating:
        - https://www.skygroup.jp/security-info/news/170308.html
    5. [CVE-2025-54253] Please refer to the official instructions for updating:
        - https://helpx.adobe.com/security/products/aem-forms/apsb25-82.html
    6. [CVE-2025-42937] Please refer to the official instructions for updating:
        - https://support.sap.com/en/my-support/knowledge-base/security-notes-news/october-2025.html

---

Computer and Communications Center
Network Systems Group