Date Posted: 2025/10/14

[Vulnerability Alert] CISA Adds 9 Known Exploited Vulnerabilities to KEV Catalog (2025/10/06-2025/10/12)

- Subject: [Vulnerability Alert] CISA Adds 9 Known Exploited Vulnerabilities to KEV Catalog (2025/10/06-2025/10/12)
- Content:
  - Forwarded from Taiwan Computer Network Emergency Response Team/Coordination Center TWCERTCC-200-202510-00000004

1. [CVE-2021-22555] Linux Kernel Heap Out-of-Bounds Write Vulnerability (CVSS v3.1: 8.3)
   - [Exploited by ransomware: Unknown] The Linux kernel has a Heap Out-of-Bounds Write vulnerability that an attacker can exploit through user namespaces to elevate privileges or cause a DoS (via heap memory corruption).
   - [Affected Platforms] Linux Kernel versions from 2.6.19-rc1 (inclusive) and later.
2. [CVE-2010-3962] Microsoft Internet Explorer Uninitialized Memory Corruption Vulnerability (CVSS v3.1: 8.1)
   - [Exploited by ransomware: Unknown] Microsoft Internet Explorer has an Uninitialized Memory Corruption vulnerability that may allow remote code execution.
   - [Affected Platforms] Please refer to the official list of affected versions.
   - https://learn.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-090
3. [CVE-2021-43226] Microsoft Windows Privilege Escalation Vulnerability (CVSS v3.1: 7.8)
   - [Exploited by ransomware: Known] Microsoft Windows Common Log File System Driver has a Privilege Escalation vulnerability that may allow a local privileged attacker to bypass specific security mechanisms.
   - [Affected Platforms] Please refer to the official list of affected versions.
   - https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-43226
4. [CVE-2013-3918] Microsoft Windows Out-of-Bounds Write Vulnerability (CVSS v3.1: 8.8)
   - [Exploited by ransomware: Unknown] Microsoft Windows has an Out-of-Bounds Write vulnerability in the ActiveX control (icardie.dll) of the InformationCardSigninHelper class. An attacker can exploit this vulnerability through a specially crafted web page. When a user browses this page, the vulnerability may lead to remote code execution. A successful attacker can obtain the same privileges as the current user. 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 list of affected versions.
   - https://learn.microsoft.com/en-us/security-updates/securitybulletins/2013/ms13-090
5. [CVE-2011-3402] Microsoft Windows Remote Code Execution Vulnerability (CVSS v3.1: 8.8)
   - [Exploited by ransomware: Unknown] Microsoft Windows Kernel has a vulnerability in the TrueType font parsing engine in the kernel-mode driver win32k.sys that may allow a remote attacker to execute arbitrary code in a Word document or web page through specially crafted font data.
   - [Affected Platforms] Please refer to the official list of affected versions.

        - https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2011/ms11-087
    6. [CVE-2010-3765] Mozilla Multiple Products Remote Code Execution Vulnerability (CVSS v3.1: 9.8)
        - [Exploited by ransomware: Unknown] Mozilla Firefox, SeaMonkey, and Thunderbird have an unspecified vulnerability when JavaScript is enabled. A remote attacker can cause memory corruption via attack vectors related to nsCSSFrameConstructor::ContentAppended, the appendChild method, incorrect index tracking, and creation of multiple frames, which may lead to arbitrary code execution.
        - [Affected Platforms] Please refer to the official list of affected versions.
        - https://blog.mozilla.org/security/2010/10/26/critical-vulnerability-in-firefox-3-5-and-firefox-3-6/
    7. [CVE-2025-61882] Oracle E-Business Suite Unspecified Vulnerability (CVSS v3.1: 9.8)
        - [Exploited by ransomware: Yes] Oracle E-Business Suite's BI Publisher integration component has an unspecified vulnerability that may allow an unauthenticated attacker to access it via an HTTP network, which may lead to compromise and takeover of Oracle Concurrent Processing.
        - [Affected Platforms] Please refer to the official list of affected versions.
        - https://www.oracle.com/security-alerts/alert-cve-2025-61882.html
    8. [CVE-2025-27915] Synacor Zimbra Collaboration Suite (ZCS) Cross-site Scripting Vulnerability (CVSS v3.1: 5.4)
        - [Exploited by ransomware: Unknown] Synacor Zimbra Collaboration Suite (ZCS) has a Cross-site Scripting vulnerability in the Classic Web UI in versions before 9.0.
        - [Affected Platforms] ZCS versions before 9.0
        - https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories
    9. [CVE-2025-27916] Synacor Zimbra Collaboration Suite (ZCS) Unrestricted Upload of File with Dangerous Type Vulnerability (CVSS v3.1: 6.5)
        - [Exploited by ransomware: Unknown] Synacor Zimbra Collaboration Suite (ZCS) has an Unrestricted Upload of File with Dangerous Type vulnerability that may allow a remote attacker to upload arbitrary files with dangerous types.
        - [Affected Platforms] Please refer to the official list of affected versions.
        - https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories

- Affected Platforms:
    - Details are in the Affected Platforms section of the Content Description
- Recommended Action:
    1. [CVE-2021-22555] The official vendor has released a fix for the vulnerability. Please update to the relevant version.
        - (1). https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/net/netfilter/x_tables.c?id=9fa492cdc160cd27ce1046cb36f47d3b2b1efa21
        - (2). https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/net/netfilter/x_tables.c?id=b29c457a6511435960115c0f548c4360d5f4801d
    2. [CVE-2010-3962] The official vendor has released a fix for the vulnerability. Please update to the relevant version.
        - https://learn.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-090
    3. [CVE-2021-43226] The official vendor has released a fix for the vulnerability. Please update to the relevant version.
        - https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-43226
    4. [CVE-2013-3918] The official vendor has released a fix for the vulnerability. Please update

to the relevant version.
   - https://learn.microsoft.com/en-us/security-updates/securitybulletins/2013/ms13-090
5. [CVE-2011-3402] The official vendor has released a fix for the vulnerability. Please update to the relevant version.
   - https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2011/ms11-087
6. [CVE-2010-3765] The official vendor has released a fix for the vulnerability. Please update to the relevant version.
   - https://blog.mozilla.org/security/2010/10/26/critical-vulnerability-in-firefox-3-5-and-firefox-3-6/
7. [CVE-2025-61882] The official vendor has released a fix for the vulnerability. Please update to the relevant version.
   - https://www.oracle.com/security-alerts/alert-cve-2025-61882.html
8. [CVE-2025-27915] The official vendor has released a fix for the vulnerability. Please update to the relevant version.
   - https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories
9. [CVE-2025-27916] The official vendor has released a fix for the vulnerability. Please update to the relevant version.
   - https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories

- References:
  1. https://www.twcert.org.tw/tw/cp-169-10419-72535-1.html

Computer and Communications Center
Network Systems Group