Date Posted: 2026/02/25

[Vulnerability Alert] CISA Adds 11 Known Exploited Vulnerabilities to KEV Catalog (2026/02/09-2026/02/15)

- Subject Explanation: [Vulnerability Alert] CISA Adds 11 Known Exploited Vulnerabilities to KEV Catalog (2026/02/09-2026/02/15)

- Content Description:
  - Forwarding Taiwan Computer Emergency Response Team / Coordination Center (TWCERT/CC) Security Alert TWCERTCC-200-202602-00000009
  - [CVE-2026-21513] Microsoft MSHTML Framework Protection Mechanism Failure Vulnerability (CVSS v3.1: 8.8)
  - [Ransomware Usage: Unknown] Microsoft MSHTML Framework contains a protection mechanism failure vulnerability, which may allow an unauthorized attacker to bypass security features over a network.
  - [CVE-2026-21525] Microsoft Windows NULL Pointer Dereference Vulnerability (CVSS v3.1: 6.2)
  - [Ransomware Usage: Unknown] Microsoft Windows Remote Access Connection Manager contains a NULL pointer dereference vulnerability, which may allow an unauthorized attacker to cause a denial of service locally.
  - [CVE-2026-21510] Microsoft Windows Shell Protection Mechanism Failure Vulnerability (CVSS v3.1: 8.8)
  - [Ransomware Usage: Unknown] Microsoft Windows Shell contains a protection mechanism failure vulnerability, which may allow an unauthorized attacker to bypass security features over a network.
  - [CVE-2026-21533] Microsoft Windows Improper Privilege Management Vulnerability (CVSS v3.1: 7.8)
  - [Ransomware Usage: Unknown] Microsoft Windows Remote Desktop Services contains an improper privilege management vulnerability, which may allow an authenticated attacker to elevate privileges locally.
  - [CVE-2026-21519] Microsoft Windows Type Confusion Vulnerability (CVSS v3.1: 7.8)
  - [Ransomware Usage: Unknown] Microsoft Desktop Windows Manager contains a type confusion vulnerability, which may allow an authenticated attacker to elevate privileges locally.
  - [CVE-2026-21514] Microsoft Office Word Reliance on Untrusted Inputs in a Security Decision Vulnerability (CVSS v3.1: 7.8)
  - [Ransomware Usage: Unknown] Microsoft Office Word contains a reliance on untrusted inputs in a security decision vulnerability, which may allow an authenticated attacker to elevate privileges locally.
  - [CVE-2026-20700] Apple Multiple Buffer Overflow Vulnerability (CVSS v3.1: 7.8)
  - [Ransomware Usage: Unknown] Apple iOS, macOS, tvOS, watchOS, and visionOS contain multiple buffer overflow vulnerabilities, which may allow an attacker with memory write permissions to execute arbitrary code.
  - [CVE-2024-43468] Microsoft Configuration Manager SQL Injection Vulnerability (CVSS

v3.1: 9.8)
    - [Ransomware Usage: Unknown] Microsoft Configuration Manager contains a SQL injection vulnerability. An unauthenticated attacker could execute commands on the server and/or the underlying database by sending a specially crafted request to the target environment.
    - [CVE-2025-15556] Notepad++ Download of Code Without Integrity Check Vulnerability (CVSS v3.1: 7.5)
    - [Ransomware Usage: Unknown] Notepad++ contains a download of code without integrity check vulnerability when using the WinGUp updater, which may allow an attacker to intercept or redirect update traffic to download and execute an installer controlled by the attacker.
    - This vulnerability may allow an attacker to execute arbitrary code with user privileges.
    - [CVE-2025-40536] SolarWinds Web Help Desk Security Control Bypass Vulnerability (CVSS v3.1: 8.1)
    - [Ransomware Usage: Unknown] SolarWinds Web Help Desk contains a security control bypass vulnerability, which may allow an unauthenticated attacker to access certain restricted functionalities.
    - [CVE-2026-1731] BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA) OS Command Injection Vulnerability (CVSS v3.1: 9.8)
    - [Ransomware Usage: Yes] BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA) contain an OS command injection vulnerability.
    - This vulnerability may allow an unauthenticated remote attacker to execute OS commands as the website user.
    - This vulnerability can be exploited without authentication or user interaction, potentially leading to system compromise, including unauthorized access, data leakage, and service disruption.
- Impacted Platforms:
    - [CVE-2026-21513] Please refer to the affected versions listed officially: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21513
    - [CVE-2026-21525] Please refer to the affected versions listed officially: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21525
    - [CVE-2026-21510] Please refer to the affected versions listed officially: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21510
    - [CVE-2026-21533] Please refer to the affected versions listed officially: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21533
    - [CVE-2026-21519] Please refer to the affected versions listed officially: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21519
    - [CVE-2026-21514] Please refer to the affected versions listed officially: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21514
    - [CVE-2026-20700] Please refer to the affected versions listed officially: https://support.apple.com/en-us/100100
    - [CVE-2024-43468] Please refer to the affected versions listed officially: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43468
    - [CVE-2025-15556] Please refer to the affected versions listed officially: https://notepad-plus-plus.org//news//clarification-security-incident/
    - [CVE-2025-40536] Please refer to the affected versions listed officially: https://www.solarwinds.com/trust-center/security-advisories/cve-2025-40536
    - [CVE-2026-1731] Please refer to the affected versions listed officially: https://www.beyondtrust.com/trust-center/security-advisories/bt26-02
- Suggested Measures:
    - [CVE-2026-21513] The official vendor has released a repair update for the vulnerability;

please update to the relevant version: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21513
- [CVE-2026-21525] The official vendor has released a repair update for the vulnerability; please update to the relevant version: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21525
- [CVE-2026-21510] The official vendor has released a repair update for the vulnerability; please update to the relevant version: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21510
- [CVE-2026-21533] The official vendor has released a repair update for the vulnerability; please update to the relevant version: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21533
- [CVE-2026-21519] The official vendor has released a repair update for the vulnerability; please update to the relevant version: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21519
- [CVE-2026-21514] The official vendor has released a repair update for the vulnerability; please update to the relevant version: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21514
- [CVE-2026-20700] The official vendor has released a repair update for the vulnerability; please update to the relevant version: https://support.apple.com/en-us/100100
- [CVE-2024-43468] The official vendor has released a repair update for the vulnerability; please update to the relevant version: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43468
- [CVE-2025-15556] The official vendor has released a repair update for the vulnerability; please update to the relevant version: https://notepad-plus-plus.org//news//clarification-security-incident/
- [CVE-2025-40536] The official vendor has released a repair update for the vulnerability; please update to the relevant version: https://www.solarwinds.com/trust-center/security-advisories/cve-2025-40536
- [CVE-2026-1731] The official vendor has released a repair update for the vulnerability; please update to the relevant version: https://www.beyondtrust.com/trust-center/security-advisories/bt26-02

Computer and Communication Center
Network Systems Division