Date Posted: 2026/03/19

[Vulnerability Alert] CISA Adds 6 Known Exploited Vulnerabilities to KEV Catalog (2026/03/09-2026/03/15)

- Subject Explanation: [Vulnerability Alert] CISA Adds 6 Known Exploited Vulnerabilities to KEV Catalog (2026/03/09-2026/03/15)

- Content Description:
  - Forwarding Taiwan Computer Emergency Response Team / Coordination Center (TWCERT/CC) Security Alert TWCERTCC-200-202603-00000014
  - [CVE-2021-22054] Omnissa Workspace ONE Server-Side Request Forgery (CVSS v3.1: 7.5)
  - [Ransomware Exploitation: Unknown] Omnissa Workspace ONE UEM contains a Server-Side Request Forgery vulnerability.
  - This vulnerability could allow a malicious attacker with network access to UEM to send requests without authentication and obtain sensitive information.
  - [CVE-2025-26399] SolarWinds Web Help Desk Deserialization of Untrusted Data Vulnerability (CVSS v3.1: 9.8)
  - [Ransomware Exploitation: Unknown] The AjaxProxy component of SolarWinds Web Help Desk contains a deserialization of untrusted data vulnerability.
  - This vulnerability could allow an attacker to execute commands on the host system.
  - [CVE-2026-1603] Ivanti Endpoint Manager (EPM) Authentication Bypass Vulnerability (CVSS v3.1: 8.6)
  - [Ransomware Exploitation: Unknown] Ivanti Endpoint Manager (EPM) contains an authentication bypass vulnerability.
  - This vulnerability could allow a remote unauthenticated attacker to leak specific stored credential data.
  - [CVE-2025-68613] n8n Improper Control of Dynamically-Managed Code Resources Vulnerability (CVSS v3.1: 9.9)
  - [Ransomware Exploitation: Unknown] The workflow expression evaluation system of n8n contains an improper control of dynamically-managed code resources vulnerability, which may lead to remote code execution.
  - [CVE-2026-3910] Google Chromium V8 Improper Restriction of Operations Within the Bounds of a Memory Buffer Vulnerability (CVSS v3.1: 8.8)
  - [Ransomware Exploitation: Unknown] Google Chromium V8 contains an improper restriction of operations within the bounds of a memory buffer vulnerability, which could allow a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
  - This vulnerability could affect multiple web browsers that use Chromium, including but not limited to Google Chrome, Microsoft Edge, and Opera.
  - [CVE-2026-3909] Google Skia Out-of-Bounds Write Vulnerability (CVSS v3.1: 8.8)
  - [Ransomware Exploitation: Unknown] Google Skia contains an out-of-bounds write vulnerability, which could allow a remote attacker to perform an out-of-bounds memory access via a crafted HTML page.
  - This vulnerability affects Google Chrome, ChromeOS, Android, Flutter, and other products

that might use Skia.

- Impacted Platforms:
  - [CVE-2021-22054] Please refer to the official list of affected versions: https://kb.omnissa.com/s/article/87167
  - [CVE-2025-26399] Please refer to the official list of affected versions: https://www.solarwinds.com/trust-center/security-advisories/cve-2025-26399
  - [CVE-2026-1603] Please refer to the official list of affected versions: https://hub.ivanti.com/s/article/Security-Advisory-EPM-February-2026-for-EPM-2024
  - [CVE-2025-68613] Please refer to the official list of affected versions: https://github.com/n8n-io/n8n/security/advisories/GHSA-v98v-ff95-f3cp
  - [CVE-2026-3910] Please refer to the official list of affected versions: https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_12.html
  - [CVE-2026-3909] Please refer to the official list of affected versions: https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_12.html
- Suggested Measures:
  - [CVE-2021-22054] Official fix updates have been released. Please update to the relevant version
  - https://kb.omnissa.com/s/article/87167
  - [CVE-2025-26399] Official fix updates have been released. Please update to the relevant version
  - https://www.solarwinds.com/trust-center/security-advisories/cve-2025-26399
  - [CVE-2026-1603] Official fix updates have been released. Please update to the relevant version
  - https://hub.ivanti.com/s/article/Security-Advisory-EPM-February-2026-for-EPM-2024
  - [CVE-2025-68613] Official fix updates have been released. Please update to the relevant version
  - https://github.com/n8n-io/n8n/security/advisories/GHSA-v98v-ff95-f3cp
  - [CVE-2026-3910] Official fix updates have been released. Please update to the relevant version
  - https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_12.html
  - [CVE-2026-3909] Official fix updates have been released. Please update to the relevant version
  - https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_12.html

---

Computer and Communication Center
Network Systems Division