Date: 2026/06/09

Vulnerability Alert CISA Adds 5 Known Exploited Vulnerabilities to KEV Catalog (2026/06/01-2026/06/07)

- Subject: Vulnerability Alert CISA Adds 5 Known Exploited Vulnerabilities to KEV Catalog (2026/06/01-2026/06/07)

- Description:
  - Forwarded from Taiwan Computer Emergency Response Team / Coordination Center Security Advisory TWCERTCC-200-202606-00000005
  - CVE-2024-21182 Oracle WebLogic Server Unspecified Vulnerability (CVSS v3.1: 7.5)
  - Known Ransomware Campaign Use: Unknown Oracle WebLogic contains an unspecified vulnerability. An unauthenticated attacker connecting via T3 or IIOP protocols could exploit this vulnerability to compromise Oracle WebLogic Server. Successful exploitation could lead to unauthorized access to critical data or grant the attacker complete access to all data accessible by Oracle WebLogic Server.
  - CVE-2022-0492 Linux Kernel Improper Authentication Vulnerability (CVSS v3.1: 7.8)
  - Known Ransomware Campaign Use: Unknown Linux Kernel contains an improper authentication vulnerability where an attacker could achieve privilege escalation through the release_agent feature of cgroups v1.
  - CVE-2025-48595 Android Framework Integer Overflow Vulnerability (CVSS v3.1: 8.4)
  - Known Ransomware Campaign Use: Unknown Android Framework contains an integer overflow vulnerability that could lead to arbitrary code execution, resulting in local privilege escalation.
  - CVE-2026-45247 Mirasvit Full Page Cache Warmer Deserialization of Untrusted Data Vulnerability (CVSS v3.1: 9.8)
  - Known Ransomware Campaign Use: Unknown Mirasvit Full Page Cache Warmer contains a deserialization of untrusted data vulnerability. An unauthenticated attacker could achieve remote code execution by providing a specially crafted PHP object within the CacheWarmer Cookie.
  - CVE-2026-28318 SolarWinds Serv-U Uncontrolled Resource Consumption Vulnerability (CVSS v3.1: 7.5)
  - Known Ransomware Campaign Use: Unknown SolarWinds Serv-U contains an uncontrolled resource consumption vulnerability. An unauthenticated attacker could cause the Serv-U service to crash by sending a specially crafted POST request using the Content-Encoding: deflate header.
- Affected Platforms:
  - CVE-2024-21182 Please refer to the official list of affected versions: https://www.oracle.com/security-alerts/cpujul2024.html
  - CVE-2022-0492 Please refer to the official list of affected versions: https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=24f6008564183aa120d07c03d9289519c2fe02af
  - CVE-2025-48595 Please refer to the official list of affected versions: https://source.android.com/docs/security/bulletin/2026/2026-06-01

    - CVE-2026-45247 Please refer to the official list of affected versions: https://mirasvit.com/package/changelog/?package=mirasvit/module-cache-warmer
    - CVE-2026-28318 Please refer to the official list of affected versions: https://www.solarwinds.com/trust-center/security-advisories/cve-2026-28318
- Mitigation Measures:
    - CVE-2024-21182 The vendor has released patches for this vulnerability. Please update to the relevant versions.
    - https://www.oracle.com/security-alerts/cpujul2024.html
    - CVE-2022-0492 The vendor has released patches for this vulnerability. Please update to the relevant versions.
    - https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=24f6008564183aa120d07c03d9289519c2fe02af
    - CVE-2025-48595 The vendor has released patches for this vulnerability. Please update to the relevant versions.
    - https://source.android.com/docs/security/bulletin/2026/2026-06-01
    - CVE-2026-45247 The vendor has released patches for this vulnerability. Please update to the relevant versions.
    - https://mirasvit.com/package/changelog/?package=mirasvit/module-cache-warmer
    - CVE-2026-28318 The vendor has released patches for this vulnerability. Please update to the relevant versions.
    - https://www.solarwinds.com/trust-center/security-advisories/cve-2026-28318

Computer and Communication Center
Network Systems Division