Post Date: 2026/05/13

【Vulnerability Alert】CISA Adds 14 Known Exploited Vulnerabilities to KEV Catalog (2026/04/20-2026/04/26) (Part 2)

- Subject: 【Vulnerability Alert】CISA Adds 14 Known Exploited Vulnerabilities to KEV Catalog (2026/04/20-2026/04/26) (Part 2)

- Description:
  - Forwarded from Taiwan Computer Emergency Response Team / Coordination Center (TWCERT/CC) Security Alert: TWCERTCC-200-202604-00000028
  - 【CVE-2024-27199】JetBrains TeamCity Relative Path Traversal Vulnerability (CVSS v3.1: 7.3)
  - 【Ransomware Exploitation: Known】 JetBrains TeamCity contains a relative path traversal vulnerability, which may lead to the ability to perform limited administrative actions.
  - 【CVE-2026-33825】Microsoft Defender Insufficient Granularity of Access Control Vulnerability (CVSS v3.1: 7.8)
  - 【Ransomware Exploitation: Unknown】 Microsoft Defender contains an insufficient granularity of access control vulnerability, which may allow an authorized attacker to perform local privilege escalation.
  - 【CVE-2026-39987】Marimo Remote Code Execution Vulnerability (CVSS v3.1: 9.8)
  - 【Ransomware Exploitation: Unknown】 Marimo contains a pre-authentication remote code execution vulnerability, allowing an unauthenticated attacker to obtain shell access and execute arbitrary system commands.
  - 【CVE-2025-29635】D-Link DIR-823X Command Injection Vulnerability (CVSS v3.1: 7.2)
  - 【Ransomware Exploitation: Unknown】 D-Link DIR-823X contains a command injection vulnerability, allowing an authorized attacker to execute arbitrary commands on the remote device by sending a POST request to /goform/set_prohibiting. Affected products may have reached End of Life (EoL) or End of Service (EoS). Users are advised to stop using this product.
  - 【CVE-2024-7399】Samsung MagicINFO 9 Server Path Traversal Vulnerability (CVSS v3.1: 8.8)
  - 【Ransomware Exploitation: Unknown】 Samsung MagicINFO 9 Server contains a path traversal vulnerability, which may allow an attacker to write arbitrary files with system privileges.
  - 【CVE-2024-57728】SimpleHelp Path Traversal Vulnerability (CVSS v3.1: 7.2)
  - 【Ransomware Exploitation: Unknown】 SimpleHelp contains a path traversal vulnerability, allowing an administrative user to upload arbitrary files to any location on the file system by uploading a specially crafted ZIP file. This vulnerability can be exploited to execute arbitrary code on the host as the SimpleHelp server user.
  - 【CVE-2024-57726】SimpleHelp Missing Authorization Vulnerability (CVSS v3.1: 9.9)
  - 【Ransomware Exploitation: Unknown】 SimpleHelp contains a missing authorization vulnerability, which may allow low-privileged technicians to create API keys with excessive permissions. These API keys can be used to escalate privileges to the server administrator role.

- Affected Platforms:
  - [CVE-2024-27199] Please refer to the official list of affected versions: https://www.jetbrains.com/privacy-security/issues-fixed/
  - [CVE-2026-33825] Please refer to the official list of affected versions: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33825
  - [CVE-2026-39987] Please refer to the official list of affected versions: https://github.com/marimo-team/marimo/security/advisories/GHSA-2679-6mx9-h9xc
  - [CVE-2025-29635] D-Link DIR-823X 240126, D-Link DIR-823X 240802
  - [CVE-2024-7399] Please refer to the official list of affected versions: https://security.samsungtv.com/securityUpdates
  - [CVE-2024-57728] Please refer to the official list of affected versions: https://guides.simple-help.com/kb---security-vulnerabilities-01-2025#security-vulnerabilities-in-simplehelp-5-5-7-and-earlier
  - [CVE-2024-57726] Please refer to the official list of affected versions: https://guides.simple-help.com/kb---security-vulnerabilities-01-2025#security-vulnerabilities-in-simplehelp-5-5-7-and-earlier
- Recommended Actions:
  - [CVE-2024-27199] Official fix updates have been released; please update to the relevant version: https://www.jetbrains.com/privacy-security/issues-fixed/
  - [CVE-2026-33825] Official fix updates have been released; please update to the relevant version: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33825
  - [CVE-2026-39987] Official fix updates have been released; please update to the relevant version: https://github.com/marimo-team/marimo/security/advisories/GHSA-2679-6mx9-h9xc
  - [CVE-2025-29635] Affected products may have reached End of Life (EoL) or End of Service (EoS); users are advised to stop using the product.
  - [CVE-2024-7399] Official fix updates have been released; please update to the relevant version: https://security.samsungtv.com/securityUpdates
  - [CVE-2024-57728] Official fix updates have been released; please update to the relevant version: https://guides.simple-help.com/kb---security-vulnerabilities-01-2025#security-vulnerabilities-in-simplehelp-5-5-7-and-earlier
  - [CVE-2024-57726] Official fix updates have been released; please update to the relevant version: https://guides.simple-help.com/kb---security-vulnerabilities-01-2025#security-vulnerabilities-in-simplehelp-5-5-7-and-earlier

---

Computer and Communication Center
Network Systems Division