Date Posted: 2026/02/10

[Vulnerability Alert] CISA Adds 6 Known Exploited Vulnerabilities to KEV Catalog (2026/02/02-2026/02/08)

- Subject Explanation: [Vulnerability Alert] CISA Adds 6 Known Exploited Vulnerabilities to KEV Catalog (2026/02/02-2026/02/08)

- Content Description:
  - Forwarding Taiwan Computer Emergency Response Team / Coordination Center (TWCERT/CC) Security Alert TWCERTCC-200-202602-00000005
  - [CVE-2021-39935] GitLab Community and Enterprise Editions Server-Side Request Forgery (SSRF) Vulnerability (CVSS v3.1: 6.8)
  - [Ransomware Usage: Unknown] GitLab Community and Enterprise editions contain a Server-Side Request Forgery (SSRF) vulnerability, which may allow unauthorized external users to execute server-side requests via the CI Lint API.
  - [CVE-2025-64328] Sangoma FreePBX OS Command Injection Vulnerability (CVSS v3.1: 7.2)
  - [Ransomware Usage: Unknown] Sangoma FreePBX Endpoint Manager contains an OS command injection vulnerability. Authenticated known users may perform command injection via the testconnection - check_ssh_connect() function, thereby remotely accessing the system as the asterisk user.
  - [CVE-2019-19006] Sangoma FreePBX Improper Authentication Vulnerability (CVSS v3.1: 9.8)
  - [Ransomware Usage: Unknown] Sangoma FreePBX contains an improper authentication vulnerability that may allow unauthorized users to bypass the password authentication mechanism and access services provided by the FreePBX administration interface.
  - [CVE-2025-40551] SolarWinds Web Help Desk Deserialization of Untrusted Data Vulnerability (CVSS v3.1: 9.8)
  - [Ransomware Usage: Unknown] SolarWinds Web Help Desk contains an untrusted data deserialization vulnerability, which may lead to remote code execution, allowing attackers to execute arbitrary commands on the host.
  - [CVE-2025-11953] React Native Community CLI OS Command Injection Vulnerability (CVSS v3.1: 9.8)
  - [Ransomware Usage: Unknown] React Native Community CLI contains an OS command injection vulnerability, which may allow unauthenticated network attackers to send POST requests to the Metro Development Server and execute arbitrary executables via vulnerable endpoints exposed by the server. In Windows environments, attackers can also execute arbitrary shell commands with fully controllable arguments.
  - [CVE-2026-24423] SmarterTools SmarterMail Missing Authentication for Critical Function Vulnerability (CVSS v3.1: 9.8)
  - [Ransomware Usage: Yes] The ConnectToHub API method in SmarterTools SmarterMail contains a missing authentication for critical function vulnerability, which may allow attackers to point the SmarterMail instance to a malicious HTTP server, potentially leading to the execution of malicious OS commands.

- Impacted Platforms:
  - [CVE-2021-39935]
  - Please refer to the affected versions listed officially: https://about.gitlab.com/releases/2021/12/06/security-release-gitlab-14-5-2-released/
  - [CVE-2025-64328]
  - Please refer to the affected versions listed officially: https://github.com/FreePBX/security-reporting/security/advisories/GHSA-vm9p-46mv-5xvw
  - [CVE-2019-19006]
  - FreePBX versions 13.0.0.0 to 13.0.197.13 (inclusive)
  - FreePBX versions 14.0.0.0 to 14.0.13.11 (inclusive)
  - FreePBX versions 15.0.0.0 to 15.0.16.26 (inclusive)