Date Posted: 2025/10/09

[Vulnerability Alert] CISA Adds 10 Known Exploited Vulnerabilities to KEV Catalog (2025/09/29-2025/10/05)

- Subject: [Vulnerability Alert] CISA Adds 10 Known Exploited Vulnerabilities to KEV Catalog (2025/09/29-2025/10/05)
- Content:
  - Forwarded from Taiwan Computer Network Emergency Response Team/Coordination Center TWCERTCC-200-202510-00000003

1. [CVE-2025-32463] Sudo Inclusion of Functionality from Untrusted Control Sphere Vulnerability (CVSS v3.1: 9.3)
   - [Exploited by ransomware: Unknown] Sudo versions before 1.9.17p1 have a vulnerability that allows a local user to gain root privileges because the /etc/nsswitch.conf file from a user-controllable directory is used when the –chroot option is specified.
   - [Affected Platforms] Please refer to the official list of affected versions
   - https://www.sudo.ws/security/advisories/chroot_bug/
2. [CVE-2025-59689] Libraesva Email Security Gateway Command Injection Vulnerability (CVSS v3.1: 6.1)
   - [Exploited by ransomware: Unknown] Libraesva Email Security Gateway (ESG) has a command injection vulnerability that allows a command injection attack to be executed via a compressed email attachment.
   - [Affected Platforms] Please refer to the official list of affected versions
   - https://docs.libraesva.com/knowledgebase/security-advisory-command-injection-vulnerability-cve-2025-59689/
3. [CVE-2025-10035] Fortra GoAnywhere MFT Deserialization of Untrusted Data Vulnerability (CVSS v3.1: 10.0)
   - [Exploited by ransomware: Known] Fortra GoAnywhere MFT has a Deserialization of Untrusted Data vulnerability that allows an attacker to forge a legitimate authorized response signature and deserialize an arbitrary object under their control, which may lead to command injection.
   - [Affected Platforms] Please refer to the official list of affected versions
   - https://www.fortra.com/security/advisories/product-security/fi-2025-012
4. [CVE-2025-20352] Cisco IOS and IOS XE Software SNMP Denial of Service and Remote Code Execution Vulnerability (CVSS v3.1: 7.7)
   - [Exploited by ransomware: Unknown] Cisco IOS and IOS XE have a stack buffer overflow vulnerability in the SNMP subsystem that may lead to Denial of Service (DoS) or Remote Code Execution.
   - [Affected Platforms] Please refer to the official list of affected versions
   - https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snmp-x4LPhte
5. [CVE-2021-21311] Adminer Server-Side Request Forgery Vulnerability (CVSS v3.1: 7.2)
   - [Exploited by ransomware: Unknown] Adminer has a Server-Side Request Forgery (SSRF) vulnerability that, if exploited, allows a remote attacker to obtain potentially sensitive information.

        - [Affected Platforms] Please refer to the official list of affected versions
        - https://github.com/vrana/adminer/security/advisories/GHSA-x5r2-hj5c-8jx6
    6. [CVE-2014-6278] GNU Bash OS Command Injection Vulnerability (CVSS v3.1: 8.8)
        - [Exploited by ransomware: Unknown] GNU Bash has an OS Command Injection vulnerability that allows a remote attacker to execute arbitrary commands via a specially crafted environment variable.
        - [Affected Platforms] GNU Bash versions 1.14 through 4.3 (inclusive)
    7. [CVE-2017-1000353] Jenkins Remote Code Execution Vulnerability (CVSS v3.1: 9.8)
        - [Exploited by ransomware: Unknown] Jenkins has a Remote Code Execution vulnerability. This vulnerability allows an attacker to transmit a serialized Java SignedObject via the remote-communication based Jenkins CLI, which will be deserialized through a new ObjectInputStream, thereby bypassing existing blocklist-based protection mechanisms.
        - [Affected Platforms] Please refer to the official list of affected versions
        - https://www.jenkins.io/security/advisory/2017-04-26/
    8. [CVE-2015-7755] Juniper ScreenOS Improper Authentication Vulnerability (CVSS v3.1: 9.8)
        - [Exploited by ransomware: Unknown] Juniper ScreenOS has an Improper Authentication vulnerability that may allow unauthorized remote administrative access to the device.
        - [Affected Platforms] Please refer to the official list of affected versions
        - https://supportportal.juniper.net/s/article/2015-12-Out-of-Cycle-Security-Bulletin-ScreenOS-Multiple-Security-issues-with-ScreenOS-CVE-2015-7755-CVE-2015-7756
    9. [CVE-2025-21043] Samsung Mobile Devices Out-of-Bounds Write Vulnerability (CVSS v3.1: 8.8)
        - [Exploited by ransomware: Unknown] Samsung Mobile Devices have an Out-of-Bounds Write vulnerability in libimagecodec.quram.so, allowing a remote attacker to execute arbitrary code.
        - [Affected Platforms] Please refer to the official list of affected versions
        - https://security.samsungmobile.com/securityUpdate.smsb
    10. [CVE-2025-4008] Smartbedded Meteobridge Command Injection Vulnerability (CVSS v3.1: 8.8)
        - [Exploited by ransomware: Unknown] Smartbedded Meteobridge has a Command Injection vulnerability that may allow an unauthenticated remote attacker to execute arbitrary commands with elevated privileges (root) on the affected device.
        - [Affected Platforms] Please refer to the official list of affected versions
        - https://forum.meteohub.de/index.php
- Affected Platforms:
    - Details are in the Affected Platforms section of the Content Description
- Recommended Action:
    1. [CVE-2025-32463] The official vendor has released a fix for the vulnerability. Please update to the relevant version.
        - https://www.sudo.ws/security/advisories/chroot_bug/
    2. [CVE-2025-59689] The official vendor has released a fix for the vulnerability. Please update to the relevant version.
        - https://docs.libraesva.com/knowledgebase/security-advisory-command-injection-vulnerability-cve-2025-59689/
    3. [CVE-2025-10035] The official vendor has released a fix for the vulnerability. Please update to the relevant version.
        - https://www.fortra.com/security/advisories/product-security/fi-2025-012
    4. [CVE-2025-20352] The official vendor has released a fix for the vulnerability. Please

update to the relevant version.
   - https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snmp-x4LPhte
5. [CVE-2021-21311] The official vendor has released a fix for the vulnerability. Please update to the relevant version.
   - https://github.com/vrana/adminer/security/advisories/GHSA-x5r2-hj5c-8jx6
6. [CVE-2014-6278] The vulnerability may affect open-source components, third-party libraries, protocols, or specific implementations. Please apply the mitigation measures released by the product vendor for patching.
7. [CVE-2017-1000353] The official vendor has released a fix for the vulnerability. Please update to the relevant version.
   - https://www.jenkins.io/security/advisory/2017-04-26/
8. [CVE-2015-7755] The official vendor has released a fix for the vulnerability. Please update to the relevant version.
   - https://supportportal.juniper.net/s/article/2015-12-Out-of-Cycle-Security-Bulletin-ScreenOS-Multiple-Security-issues-with-ScreenOS-CVE-2015-7755-CVE-2015-7756
9. [CVE-2025-21043] The official vendor has released a fix for the vulnerability. Please update to the relevant version.
   - https://security.samsungmobile.com/securityUpdate.smsb
10. [CVE-2025-4008] The official vendor has released a fix for the vulnerability. Please update to the relevant version.
   - https://forum.meteohub.de/index.php

Computer and Communications Center
Network Systems Group