Date Posted: 2025/08/05

[Vulnerability Alert] CISA Adds 3 Known Exploited Vulnerabilities to KEV Catalog (2025/07/28-2025/08/03)

- Subject: [Vulnerability Alert] CISA Adds 3 Known Exploited Vulnerabilities to KEV Catalog (2025/07/28-2025/08/03)
- Content:
  - Forwarded from Taiwan Computer Network Emergency Response Team/Coordination Center TWCERTCC-200-202508-00000001
  1. [CVE-2023-2533] PaperCut NG/MF Cross-Site Request Forgery (CSRF) Vulnerability (CVSS v3.1: 8.4)
     - [Exploited by ransomware: Unknown] PaperCut NG/MF has a cross-site request forgery vulnerability. Under specific conditions, an attacker may exploit this vulnerability to modify security settings or execute arbitrary code.
     - [Affected Platforms] Please refer to the official list of affected versions
     - https://www.papercut.com/kb/Main/SecurityBulletinJune2023
  2. [CVE-2025-20337] Cisco Identity Services Engine Injection Vulnerability (CVSS v3.1: 10.0)
     - [Exploited by ransomware: Unknown] Specific APIs in Cisco Identity Services Engine (ISE) and Cisco ISE-PIC have an injection vulnerability due to insufficient validation of user-provided input. An attacker can exploit this vulnerability by submitting a specially crafted API request. If successfully exploited, the vulnerability may allow an attacker to perform remote code execution on the affected device and obtain root privileges.
     - [Affected Platforms] Please refer to the official list of affected versions
     - https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-unauth-rce-ZAd2GnJ6
  3. [CVE-2025-20281] Cisco Identity Services Engine Injection Vulnerability (CVSS v3.1: 10.0)
     - [Exploited by ransomware: Unknown] Specific APIs in Cisco Identity Services Engine (ISE) and Cisco ISE-PIC have an injection vulnerability due to insufficient validation of user-provided input. An attacker can exploit this vulnerability by submitting a specially crafted API request. If successfully exploited, the vulnerability may allow an attacker to perform remote code execution on the affected device and obtain root privileges.
     - [Affected Platforms] Please refer to the official list of affected versions
     - https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-unauth-rce-ZAd2GnJ6
- Affected Platforms:
  - Details are in the Affected Platforms section of the Content Description
- Recommended Action:
  1. [CVE-2023-2533] The official site has released a patch for the vulnerability, please update to the relevant version
     - https://www.papercut.com/kb/Main/SecurityBulletinJune2023
  2. [CVE-2025-20337] The official site has released a patch for the vulnerability, please update to the relevant version
     - https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco

-sa-ise-unauth-rce-ZAd2GnJ6

3. [CVE-2025-20281] The official site has released a patch for the vulnerability, please update to the relevant version
    - https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-unauth-rce-ZAd2GnJ6

Computer and Communications Center
Network Systems Group

From:
https://net.nthu.edu.tw/netsys/ - **網路系統組**

Permanent link:
https://net.nthu.edu.tw/netsys/en:mailing:announcement:20250805_02

Last update: **2025/08/05 17:11**