Posting Date: 2026/08/20

【Vulnerability Alert】CISA Adds 3 Known Exploited Vulnerabilities to KEV Catalog (2026/08/10-2026/08/16)

- Subject: 【Vulnerability Alert】CISA Adds 3 Known Exploited Vulnerabilities to KEV Catalog (2026/08/10-2026/08/16)

- Description:
  - Forwarded Cybersecurity Information Advisory from Taiwan Computer Emergency Response Team/Coordination Center (TWCERT/CC) TWCERTCC-200-202608-00000013
  - 【CVE-2026-20349】Cisco Secure Firewall Adaptive Security Appliance (ASA) and Secure Firewall Threat Defense (FTD) Heap Inspection Vulnerability (CVSS v3.1: 8.6)
  - 【Ransomware Use: Unknown】 A heap inspection vulnerability exists in Cisco Secure Firewall Adaptive Security Appliance (ASA) and Secure Firewall Threat Defense (FTD). An unauthenticated, remote attacker could exploit this vulnerability to cause an unexpected reload of the device, resulting in a denial-of-service (DoS) condition.
  - 【CVE-2026-68820】Microsoft Windows Ancillary Function Driver for WinSock Use-After-Free Vulnerability (CVSS v3.1: 7.0)
  - 【Ransomware Use: Unknown】 A use-after-free vulnerability exists in the Microsoft Windows Ancillary Function Driver for WinSock. An authorized attacker could exploit this vulnerability to elevate privileges locally.
  - 【CVE-2026-72898】Metabase SQL Injection Vulnerability (CVSS v3.1: 10.0)
  - 【Ransomware Use: Unknown】 An SQL injection vulnerability exists in Metabase. An unauthenticated, remote attacker could exploit this vulnerability to inject arbitrary SQL commands into the Metabase application database, thereby gaining administrator privileges for the instance. Once privileges are obtained, the attacker may further modify application settings, steal stored credentials for connected databases, and read or export any data accessible through these connections.
- Affected Platforms:
  - 【CVE-2026-20349】 Please refer to the affected versions listed on the official advisory: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-vpn-dos-dzv4mQFF
  - 【CVE-2026-68820】 Please refer to the affected versions listed on the official advisory: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-68820
  - 【CVE-2026-72898】 Please refer to the affected versions listed on the official advisory: https://github.com/metabase/metabase/security/advisories/GHSA-vwf4-m7j8-wcjf
- Recommendations:
  - 【CVE-2026-20349】 Official fix updates have been released for this vulnerability. Please update to the relevant version: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-vpn-dos-dzv4mQFF
  - 【CVE-2026-68820】 Official fix updates have been released for this vulnerability. Please update to the relevant version: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-68820

- CVE-2026-72898 Official fix updates have been released for this vulnerability. Please update to the relevant version: https://github.com/metabase/metabase/security/advisories/GHSA-vwf4-m7j8-wcjf

---

Computer and Communication Center
Network System Division Sincerely

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

Permanent link:
https://net.nthu.edu.tw/netsys/en:mailing:announcement:20260820_21

Last update: **2026/08/20 11:34**