Date Posted: 2026/07/24 \

【Vulnerability Alert】CISA Adds 10 Known Exploited Vulnerabilities to KEV Catalog (2026/07/13-2026/07/19)

- Subject: 【Vulnerability Alert】CISA Adds 10 Known Exploited Vulnerabilities to KEV Catalog (2026/07/13-2026/07/19)

\

- Description:
  - Forwarded Cybersecurity Alert from Taiwan Computer Emergency Response Team/Coordination Center TWCERTCC-200-202607-00000011
  - 【CVE-2008-4128】Cisco IOS Cross-Site Request Forgery Vulnerability (CVSS v3.1: 4.3)
  - 【Known Ransomware Use: Unknown】 Multiple cross-site request forgery (CSRF) vulnerabilities in the HTTP Administration component in Cisco IOS 12.4 used by Cisco 871 Integrated Services Router allow remote attackers to execute arbitrary commands on the affected device by enticing users to send crafted requests.
  - 【CVE-2026-56155】Microsoft Active Directory Federation Services Insufficient Granularity of Access Control Vulnerability (CVSS v3.1: 7.8)
  - 【Known Ransomware Use: Unknown】 Microsoft Active Directory Federation Services contains an insufficient granularity of access control vulnerability that allows an authorized attacker to escalate privileges locally.
  - 【CVE-2026-56164】Microsoft SharePoint Server Missing Authentication for Critical Function Vulnerability (CVSS v3.1: 5.3)
  - 【Known Ransomware Use: Unknown】 Microsoft SharePoint Server contains a missing authentication for critical function vulnerability that allows an unauthorized attacker to escalate privileges over a network.
  - 【CVE-2026-15409】SonicWall SMA1000 Appliances Server-Side Request Forgery Vulnerability (CVSS v3.1: 10.0)
  - 【Known Ransomware Use: Unknown】 SonicWall SMA1000 Appliances contain a server-side request forgery (SSRF) vulnerability that could allow an unauthenticated remote attacker to cause the appliance to send requests to an unintended destination.
  - 【CVE-2026-15410】SonicWall SMA1000 Appliances Code Injection Vulnerability (CVSS v3.1: 7.2)
  - 【Known Ransomware Use: Unknown】 SonicWall SMA1000 Appliances contain a code injection vulnerability that, under specific conditions, could allow an authenticated remote attacker with administrator privileges to execute arbitrary operating system commands.
  - 【CVE-2026-46817】Oracle E-Business Suite Improper Privilege Management Vulnerability (CVSS v3.1: 9.8)
  - 【Known Ransomware Use: Unknown】 Oracle E-Business Suite contains an improper privilege management vulnerability that allows an unauthenticated attacker with network access via HTTP to compromise Oracle Payments. Successful exploitation may result in the takeover of Oracle Payments.
  - 【CVE-2023-4346】KNX Association KNX Protocol Connection Authorization Option 1 Overly Restrictive Account Lockout Mechanism Vulnerability (CVSS v3.1: 7.5)
  - 【Known Ransomware Use: Unknown】 KNX Association KNX Protocol Connection

Authorization Option 1 contains an improper account lockout mechanism vulnerability that could allow an attacker to erase all devices without additional security options enabled and set a BCU key to lock the devices.
  - 【CVE-2026-58644】Microsoft SharePoint Server Deserialization of Untrusted Data Vulnerability (CVSS v3.1: 9.8)
  - 【Known Ransomware Use: Unknown】 Microsoft SharePoint Server contains a deserialization of untrusted data vulnerability that could allow an unauthorized attacker to execute code over a network.
  - 【CVE-2026-25089】Fortinet FortiSandbox OS Command Injection Vulnerability (CVSS v3.1: 9.8)
  - 【Known Ransomware Use: Unknown】 An OS command injection vulnerability in the Web UI of Fortinet FortiSandbox, FortiSandbox Cloud, and FortiSandbox PaaS may allow an unauthenticated attacker to execute unauthorized commands via specially crafted HTTP requests.
  - 【CVE-2026-39808】Fortinet FortiSandbox OS Command Injection Vulnerability (CVSS v3.1: 9.8)
  - 【Known Ransomware Use: Unknown】 An OS command injection vulnerability in the API endpoint of Fortinet FortiSandbox may allow an unauthenticated attacker to execute unauthorized code or commands via specially crafted HTTP requests.
- Affected Platforms:
  - 【CVE-2008-4128】Cisco IOS 12.4 used by Cisco 871 Integrated Services Router, involving the HTTP Administration component.
  - 【CVE-2026-56155】Please refer to the official vendor page for affected versions: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-56155
  - 【CVE-2026-56164】Please refer to the official vendor page for affected versions: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-56164
  - 【CVE-2026-15409】Please refer to the official vendor page for affected versions: https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0008
  - 【CVE-2026-15410】Please refer to the official vendor page for affected versions: https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0008
  - 【CVE-2026-46817】Please refer to the official vendor page for affected versions: https://www.oracle.com/security-alerts/cspumay2026.html
  - 【CVE-2023-4346】Please refer to the official advisory for affected versions: https://www.cisa.gov/news-events/ics-advisories/icsa-23-236-01
  - 【CVE-2026-58644】Please refer to the official vendor page for affected versions: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-58644
  - 【CVE-2026-25089】Please refer to the official vendor page for affected versions: https://fortiguard.fortinet.com/psirt/FG-IR-26-141
  - 【CVE-2026-39808】Please refer to the official vendor page for affected versions: https://fortiguard.fortinet.com/psirt/FG-IR-26-100
- Recommendation:
  - 【CVE-2008-4128】 Affected products may have reached End of Life (EoL) and/or End of Service (EoS). Users are advised to discontinue using the product. https://www.cisco.com/c/en/us/obsolete/ios-nx-os-software/cisco-ios-software-releases-12-4-mainline.html
  - 【CVE-2026-56155】 Security updates have been released by the vendor. Please update to the relevant version: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-56155
  - 【CVE-2026-56164】 Security updates have been released by the vendor. Please update to the relevant version:

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-56164
- CVE-2026-15409 Security updates have been released by the vendor. Please update to the relevant version: https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0008
- CVE-2026-15410 Security updates have been released by the vendor. Please update to the relevant version: https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0008
- CVE-2026-46817 Security updates have been released by the vendor. Please update to the relevant version: https://www.oracle.com/security-alerts/cspumay2026.html
- CVE-2023-4346 Mitigation measures have been released by the vendor: https://www.cisa.gov/news-events/ics-advisories/icsa-23-236-01
- CVE-2026-58644 Security updates have been released by the vendor. Please update to the relevant version: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-58644
- CVE-2026-25089 Security updates have been released by the vendor. Please update to the relevant version: https://fortiguard.fortinet.com/psirt/FG-IR-26-141
- CVE-2026-39808 Security updates have been released by the vendor. Please update to the relevant version: https://fortiguard.fortinet.com/psirt/FG-IR-26-100

Computer and Communication Center \ Network System Division

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

Permanent link:
https://net.nthu.edu.tw/netsys/en:mailing:announcement:20260724_21

Last update: **2026/07/24 10:18**