POSTING DATE: 2025/12/29

[VULNERABILITY ALERT] CISA Adds 7 Known Exploited Vulnerabilities to KEV Catalog (2025/12/15-2025/12/21)

- Subject: [VULNERABILITY ALERT] CISA Adds 7 Known Exploited Vulnerabilities to KEV Catalog (2025/12/15-2025/12/21)

- Content Description:
  - Forwarded from Taiwan Computer Emergency Response Team/Coordination Center Security Alert TWCERTCC-200-202512-00000011
  - [CVE-2025-14611] Gladinet CentreStack and Triofox Hard Coded Cryptographic Vulnerability (CVSS v3.1: 9.8)
  - [Known to be exploited by ransomware: Unknown] Gladinet CentreStack and TrioFox contain a hard-coded cryptographic key vulnerability due to the implementation of their AES encryption scheme.
  - This vulnerability reduces the security of publicly exposed endpoints. If a specially crafted request is received without authentication, it may be affected by arbitrary local file inclusion.
  - [CVE-2025-43529] Apple Multiple Products Use-After-Free WebKit Vulnerability (CVSS v3.1: 8.8)
  - [Known to be exploited by ransomware: Unknown] A use-after-free vulnerability exists in WebKit within Apple iOS, iPadOS, macOS, and other Apple products. Processing maliciously designed web content may lead to memory corruption.
  - This vulnerability may affect all HTML parsers using WebKit, including but not limited to Apple Safari and other non-Apple products that rely on WebKit for HTML processing.
  - [CVE-2025-59718] Fortinet Multiple Products Improper Verification of Cryptographic Signature Vulnerability (CVSS v3.1: 9.8)
  - [Known to be exploited by ransomware: Unknown] Fortinet FortiOS, FortiSwitchMaster, FortiProxy, and FortiWeb contain an improper verification of cryptographic signature vulnerability.
  - This vulnerability may allow an unauthenticated attacker to bypass FortiCloud SSO login authentication via a specially crafted SAML message. Please note that CVE-2025-59719 involves the same issue and was mentioned in the same vendor advisory. Be sure to apply all patches listed in that advisory.
  - [CVE-2025-59374] ASUS Live Update Embedded Malicious Code Vulnerability (CVSS v3.1: 9.8)
  - [Known to be exploited by ransomware: Unknown] ASUS Live Update contains an embedded malicious code vulnerability. The client was modified and released without authorization after the supply chain was compromised.
  - The modified version may cause devices meeting specific target conditions to perform unexpected behaviors. Affected products may have reached End of Life (EoL) and/or End of Service (EoS). Users are advised to stop using the product immediately.
  - [CVE-2025-40602] SonicWall SMA1000 Missing Authorization Vulnerability (CVSS v3.1: 6.6)

    - [Known to be exploited by ransomware: Unknown] SonicWall SMA1000 contains a missing authorization vulnerability, which may lead to privilege escalation in the affected device's Appliance Management Console (AMC).
    - [CVE-2025-20393] Cisco Multiple Products Improper Input Validation Vulnerability (CVSS v3.1: 10.0)
    - [Known to be exploited by ransomware: Unknown] An improper input validation vulnerability exists in Cisco Secure Email Gateway, Secure Email, AsyncOS software, and Web Manager appliances. This vulnerability may allow a threat actor to execute arbitrary commands with root privileges on the underlying operating system of the affected device.
    - [CVE-2025-14733] WatchGuard Firebox Out of Bounds Write Vulnerability (CVSS v3.1: 9.8)
    - [Known to be exploited by ransomware: Unknown] The iked process of WatchGuard Fireware OS contains an out-of-bounds write vulnerability.
    - This vulnerability may allow an unauthenticated remote attacker to execute arbitrary code and affects Mobile VPN with IKEv2 and Branch Office VPN with IKEv2 configured with a dynamic gateway peer.
- Affected Platforms:
    - [CVE-2025-14611] Gladinet CentreStack versions prior to 16.12.10420.56791 (exclusive); Gladinet Triofox versions prior to 16.12.10420.56791 (exclusive)
    - [CVE-2025-43529] Please refer to the affected versions listed by the official source: https://support.apple.com/en-us/125884
    - https://support.apple.com/en-us/125885
    - https://support.apple.com/en-us/125886
    - https://support.apple.com/en-us/125889
    - https://support.apple.com/en-us/125890
    - https://support.apple.com/en-us/125891
    - https://support.apple.com/en-us/125892
    - [CVE-2025-59718] Please refer to the affected versions listed by the official source: https://fortiguard.fortinet.com/psirt/FG-IR-25-647
    - [CVE-2025-59374] Please refer to the affected versions listed by the official source: https://www.asus.com/news/hqfgvuyz6uyayje1/
    - [CVE-2025-40602] Please refer to the affected versions listed by the official source: https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0019
    - [CVE-2025-20393] Please refer to the affected versions listed by the official source: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sma-attack-N9bf4
    - [CVE-2025-14733] Please refer to the affected versions listed by the official source: https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2025-00027
- Recommended Actions:
    - [CVE-2025-14611] Upgrade corresponding products to the following versions (or higher): Gladinet CentreStack 16.12.10420.56791, Gladinet Triofox 16.12.10420.56791
    - [CVE-2025-43529] The vendor has released security updates for this vulnerability; please update to the relevant versions:
    - https://support.apple.com/en-us/125884
    - https://support.apple.com/en-us/125885
    - https://support.apple.com/en-us/125886
    - https://support.apple.com/en-us/125889
    - https://support.apple.com/en-us/125890
    - https://support.apple.com/en-us/125891
    - https://support.apple.com/en-us/125892
    - [CVE-2025-59718] The vendor has released security updates for this vulnerability; please

update to the relevant versions: https://fortiguard.fortinet.com/psirt/FG-IR-25-647
- [CVE-2025-59374] The vendor has released security updates for this vulnerability; please update to the relevant versions: https://www.asus.com/news/hqfgvuyz6uyayje1/
- [CVE-2025-40602] The vendor has released security updates for this vulnerability; please update to the relevant versions: https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0019
- [CVE-2025-20393] The vendor has released security updates for this vulnerability; please update to the relevant versions: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sma-attack-N9bf4
- [CVE-2025-14733] The vendor has released security updates for this vulnerability; please update to the relevant versions: https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2025-00027

Computer and Communication Center
Network Systems Division, Respectfully