Date Posted: 2026/03/11

[Vulnerability Alert] CISA Adds 7 Known Exploited Vulnerabilities to KEV Catalog (2026/03/02-2026/03/08)

- Subject Explanation: [Vulnerability Alert] CISA Adds 7 Known Exploited Vulnerabilities to KEV Catalog (2026/03/02-2026/03/08)

- Content Description:
  - Forwarding Taiwan Computer Emergency Response Team / Coordination Center (TWCERT/CC) Security Alert TWCERTCC-200-202603-00000007
  - [CVE-2026-22719] Broadcom VMware Aria Operations Command Injection Vulnerability (CVSS v3.1: 8.1)
  - [Ransomware Exploitation: Unknown] Broadcom VMware Aria Operations contains a command injection vulnerability. An unauthenticated attacker could exploit this vulnerability to execute arbitrary commands, which could lead to remote code execution when supporting assistive product migration.
  - [CVE-2026-21385] Qualcomm Multiple Chipsets Memory Corruption Vulnerability (CVSS v3.1: 7.8)
  - [Ransomware Exploitation: Unknown] Multiple Qualcomm chipsets contain a memory corruption vulnerability during memory allocation alignment.
  - [CVE-2017-7921] Hikvision Multiple Products Improper Authentication Vulnerability (CVSS v3.1: 9.8)
  - [Ransomware Exploitation: Unknown] Multiple Hikvision products contain an improper authentication vulnerability. A malicious user could exploit this to escalate system privileges and access sensitive information.
  - [CVE-2021-22681] Rockwell Multiple Products Insufficient Protected Credentials Vulnerability (CVSS v3.1: 9.8)
  - [Ransomware Exploitation: Unknown] Multiple Rockwell products contain an insufficient protected credentials vulnerability. A key in the Studio 5000 Logix Designer software could be discovered, which is used to authenticate communications between Logix controllers and Rockwell Automation design software. If successfully exploited, an unauthorized application could connect to a Logix controller.
  - [CVE-2023-43000] Apple Multiple products Use-After-Free Vulnerability (CVSS v3.1: 8.8)
  - [Ransomware Exploitation: Unknown] Apple macOS, iOS, iPadOS, and Safari 16.6 contain a use-after-free vulnerability. When the system processes maliciously crafted web content, it may lead to memory corruption.
  - [CVE-2021-30952] Apple Multiple Products Integer Overflow or Wraparound Vulnerability (CVSS v3.1: 8.8)
  - [Ransomware Exploitation: Unknown] Apple tvOS, macOS, Safari, iPadOS, and watchOS contain an integer overflow or wraparound vulnerability. When the system processes maliciously crafted web content, it may lead to arbitrary code execution.
  - [CVE-2023-41974] Apple iOS and iPadOS Use-After-Free Vulnerability (CVSS v3.1: 7.8)
  - [Ransomware Exploitation: Unknown] Apple iOS and iPadOS contain a use-after-free vulnerability. An application could exploit this to execute arbitrary code with kernel

privileges.

- Impacted Platforms:
  - [CVE-2026-22719] Please refer to the official list of affected versions
  - https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36947
  - [CVE-2026-21385] Please refer to the official list of affected versions
  - https://docs.qualcomm.com/securitybulletin/march-2026-bulletin.html
  - [CVE-2017-7921] Please refer to the official list of affected versions
  - https://www.hikvision.com/us-en/support/document-center/special-notices/privilege-escalating-vulnerability-in-certain-hikvision-ip-cameras/
  - [CVE-2021-22681] Please refer to the official list of affected versions
  - https://www.cisa.gov/news-events/ics-advisories/icsa-21-056-03
  - [CVE-2023-43000] Please refer to the official list of affected versions
  - https://support.apple.com/en-us/120324
  - https://support.apple.com/en-us/120331
  - https://support.apple.com/en-us/120338
  - [CVE-2021-30952] Please refer to the official list of affected versions
  - https://support.apple.com/en-us/HT212975
  - https://support.apple.com/en-us/HT212976
  - https://support.apple.com/en-us/HT212978
  - https://support.apple.com/en-us/HT212980
  - https://support.apple.com/en-us/HT212982
  - [CVE-2023-41974] Please refer to the official list of affected versions
  - https://support.apple.com/en-us/HT213938
- Suggested Measures:
  - [CVE-2026-22719] Official fix updates have been released. Please update to the relevant version
  - https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36947
  - [CVE-2026-21385] Official fix updates have been released. Please update to the relevant version
  - https://docs.qualcomm.com/securitybulletin/march-2026-bulletin.html
  - [CVE-2017-7921] Official fix updates have been released. Please update to the relevant version
  - https://www.hikvision.com/us-en/support/document-center/special-notices/privilege-escalating-vulnerability-in-certain-hikvision-ip-cameras/
  - [CVE-2021-22681] Official fix updates have been released. Please update to the relevant version
  - https://www.cisa.gov/news-events/ics-advisories/icsa-21-056-03
  - [CVE-2023-43000] Official fix updates have been released. Please update to the relevant version
  - https://support.apple.com/en-us/120324
  - https://support.apple.com/en-us/120331
  - https://support.apple.com/en-us/120338
  - [CVE-2021-30952] Official fix updates have been released. Please update to the relevant version
  - https://support.apple.com/en-us/HT212975
  - https://support.apple.com/en-us/HT212976
  - https://support.apple.com/en-us/HT212978
  - https://support.apple.com/en-us/HT212980

- https://support.apple.com/en-us/HT212982
- [CVE-2023-41974] Official fix updates have been released. Please update to the relevant version
- https://support.apple.com/en-us/HT213938

Computer and Communication Center
Network Systems Division