

Posting Date: 2026/10/08

□Vulnerability Alert□CISA Adds 6 Known Exploited Vulnerabilities to the KEV Catalog (2026/09/28-2026/10/04)

- Subject:□Vulnerability Alert□CISA Adds 6 Known Exploited Vulnerabilities to the KEV Catalog (2026/09/28-2026/10/04)
- Description:
 - Forwarded TWCERT/CC (Taiwan Computer Emergency Response Team and Coordination Center) Security Alert TWCERTCC-200-202610-00000002
 - □CVE-2026-86950□Apple Multiple Products Out-of-Bounds Write Vulnerability (CVSS v3.1: 8.8)
 - □Exploited by Ransomware:Unknown□ Apple iOS, macOS and iPadOS have an out-of-bounds write vulnerability in CoreGraphics that may lead to arbitrary code execution.
 - □CVE-2026-76504□Cisco Catalyst SD-WAN Manager Hex Encoding Vulnerability (CVSS v3.1: 9.8)
 - □Exploited by Ransomware:Unknown□ Cisco Catalyst SD-WAN Manager has a hex encoding vulnerability. Due to improper handling of URI encoding in HTTP requests, an unauthenticated remote attacker may exploit this vulnerability to access the affected systems with administrator privileges.
 - □CVE-2026-104286□Fortinet FortiMail Path Traversal Vulnerability (CVSS v3.1: 9.8)
 - □Exploited by Ransomware:Unknown□ Fortinet FortiMail has a path traversal vulnerability that may allow an unauthenticated attacker to write arbitrary files to the underlying system through specially crafted HTTP or HTTPS requests.
 - □CVE-2026-102490□Zammad GmbH Zammad Improper Privilege Management Vulnerability (CVSS v3.1: 9.8)
 - □Exploited by Ransomware:Unknown□ Zammad GmbH Zammad has an improper privilege management vulnerability that may allow a local zammad user to escalate privileges to root.
 - □CVE-2026-102489□Zammad GmbH Zammad Session Fixation Vulnerability (CVSS v3.1: 9.8)
 - □Exploited by Ransomware:Unknown□ Zammad GmbH Zammad has a Session Fixation vulnerability that may allow an attacker to remotely execute arbitrary code as the zammad user.
 - □CVE-2026-88779□Citrix NetScaler Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability (CVSS v4.0: 8.7)
 - □Exploited by Ransomware:Unknown□ Citrix NetScaler ADC and Citrix NetScaler Gateway have an improper restriction of operations within the bounds of a memory buffer vulnerability that may lead to denial of service.
- Affected Platforms:
 - □CVE-2026-86950□Please refer to the affected versions listed by the vendor <https://support.apple.com/en-us/100100>
 - □CVE-2026-76504□Please refer to the affected versions listed by the vendor <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd>

[wan-webauth-xr8beuuU](#)

- [CVE-2026-104286](#) Please refer to the affected versions listed by the vendor <https://fortiguard.fortinet.com/psirt/FG-IR-26-175>
- [CVE-2026-102490](#) Please refer to the affected versions listed by the vendor <https://csirt.divd.nl/cves/CVE-2026-102490/>
- [CVE-2026-102489](#) Please refer to the affected versions listed by the vendor <https://csirt.divd.nl/cves/CVE-2026-102489/>
- [CVE-2026-88779](#) Please refer to the affected versions listed by the vendor <https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697174>
- Recommended Actions:
 - [CVE-2026-86950](#) The vendor has released a fix update for the vulnerability. Please update to the relevant version <https://support.apple.com/en-us/100100>
 - [CVE-2026-76504](#) The vendor has released a fix update for the vulnerability. Please update to the relevant version <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-webauth-xr8beuuU>
 - [CVE-2026-104286](#) The vendor has released a fix update for the vulnerability. Please update to the relevant version <https://fortiguard.fortinet.com/psirt/FG-IR-26-175>
 - [CVE-2026-102490](#) The vendor has released a fix update for the vulnerability. Please update to the relevant version <https://community.zammad.org/t/take-care-local-privilege-escalation-cve-2026-102490-is-reported-as-being-actively-exploited/21297/2>
 - [CVE-2026-102489](#) The vendor has released a fix update for the vulnerability. Please update to the relevant version <https://community.zammad.org/t/take-care-local-privilege-escalation-cve-2026-102490-is-reported-as-being-actively-exploited/21297/2>
 - [CVE-2026-88779](#) The vendor has released a fix update for the vulnerability. Please update to the relevant version <https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697174>
- References:

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:20261008_21



Last update: **2026/10/08 08:42**