# 🛡️ Weekly IT Security Brief (Official-source-first) | 2026-03-22 06:01

Formatted for readability · Auto-generated

## 📌 Weekly Summary

- Priority snapshot: 8 KEV-listed vulnerabilities are actively exploited in the wild (top 8 shown in this brief).
- Urgent patch focus: CVE-2025-32432(2026-04-03), CVE-2025-54068(2026-04-03), CVE-2025-43510(2026-04-03). Prioritize internet-facing and privileged systems first.
- Threat trend #1: CTI-REALM: A new benchmark for end-to-end detection rule generation with AI agents. CTI-REALM: A new benchmark for end-to-end detection rule generation with AI agents
- Threat trend #2: Secure agentic AI end-to-end. Secure agentic AI end-to-end
- Recommended action this week: patch KEV/high-risk exposed services within 24 hours and tighten monitoring for anomalous login, command execution, and credential access patterns.

## 🔎 Report A: CVE Deep Dive (CISA KEV + NVD)

## CVE-2025-32432

| | |
|---|---|
| **CVE Title** | CVE-2025-32432 \| craftcms/craft_cms \| Remote Code Execution |
| **CVE Description** | Craft is a flexible, user-friendly CMS for creating custom digital experiences on the web and beyond. Starting from version 3.0.0-RC1 to before 3.9.15, 4.0.0-RC1 to before 4.14.15, and 5.0.0-RC1 to before 5.6.17, Craft is vulnerable to remote code execution. This is a high-impact, low-complexity attack vector. This issue has been patched in versions 3.9.15, 4.14.15, and 5.6.17, and is an additional fix for CVE-2023-... |
| **Root Cause** | Unsafe deserialization or input-handling flaws enable arbitrary code execution. |
| **Exploitation Prerequisite** | Relevant endpoint is exposed and unpatched. |
| **Exploit Path** | Malicious request/payload -> vulnerability trigger -> remote command execution. |
| **Affected Products** | craftcms/craft_cms |
| **Risk Score** | 10.0 (CRITICAL) |
| **Exploited in the wild** | Listed in CISA KEV |
| **KEV remediation due date** | 2026-04-03 |
| **Mitigation** | Apply vendor patches immediately, reduce internet exposure, harden WAF/ACL controls, and enable anomaly detection. Since active exploitation is observed, patch high-risk assets within 24 hours. |
| **Source** | https://www.cisa.gov/known-exploited-vulnerabilities-catalog |
| **Source** | https://nvd.nist.gov/vuln/detail/CVE-2025-32432 |

## CVE-2025-54068

| | |
|---|---|
| **CVE Title** | CVE-2025-54068 \| laravel/livewire \| Unknown Type |
| **CVE Description** | Livewire is a full-stack framework for Laravel. In Livewire v3 up to and including v3.6.3, a vulnerability allows unauthenticated attackers to achieve remote command execution in specific scenarios. The issue stems from how certain component property updates are hydrated. This vulnerability is unique to Livewire v3 and does not affect prior major versions. Exploitation requires a component to be mounted and configur... |
| **Root Cause** | Authentication workflow has logical flaws allowing bypass. |
| **Exploitation Prerequisite** | Target service is network-reachable and accepts attacker-crafted unauthorized requests. |
| **Exploit Path** | Unauthorized request -> auth bypass -> sensitive data access / privileged operations. |
| **Affected Products** | laravel/livewire |
| **Risk Score** | 9.8 (CRITICAL) |
| **Exploited in the wild** | Listed in CISA KEV |
| **KEV remediation due date** | 2026-04-03 |
| **Mitigation** | Apply vendor patches immediately, reduce internet exposure, harden WAF/ACL controls, and enable anomaly detection. Since active exploitation is observed, patch high-risk assets within 24 hours. |
| **Source** | https://www.cisa.gov/known-exploited-vulnerabilities-catalog |
| **Source** | https://nvd.nist.gov/vuln/detail/CVE-2025-54068 |

## CVE-2025-43510

| | |
|---|---|
| **CVE Title** | CVE-2025-43510 \| apple/ipados \| Unknown Type |
| **CVE Description** | A memory corruption issue was addressed with improved lock state checking. This issue is fixed in watchOS 26.1, iOS 18.7.2 and iPadOS 18.7.2, macOS Tahoe 26.1, visionOS 26.1, tvOS 26.1, macOS Sonoma 14.8.2, macOS Sequoia 15.7.2, iOS 26.1 and iPadOS 26.1. A malicious application may cause unexpected changes in memory shared between processes. |
| **Root Cause** | Use vendor advisories and patch notes for authoritative technical details. |
| **Exploitation Prerequisite** | Affected version is reachable through an exploitable path and remains unpatched. |
| **Exploit Path** | Attacker leverages public PoC or observed exploit chain for intrusion. |
| **Affected Products** | apple/ipados, apple/iphone_os, apple/macos, apple/tvos, apple/visionos |
| **Risk Score** | 7.8 (HIGH) |
| **Exploited in the wild** | Listed in CISA KEV |
| **KEV remediation due date** | 2026-04-03 |
| **Mitigation** | Apply vendor patches immediately, reduce internet exposure, harden WAF/ACL controls, and enable anomaly detection. Since active exploitation is observed, patch high-risk assets within 24 hours. |
| **Source** | https://www.cisa.gov/known-exploited-vulnerabilities-catalog |
| **Source** | https://nvd.nist.gov/vuln/detail/CVE-2025-43510 |

## CVE-2025-43520

| | |
|---|---|
| **CVE Title** | CVE-2025-43520 \| apple/ipados \| Unknown Type |
| **CVE Description** | A memory corruption issue was addressed with improved memory handling. This issue is fixed in watchOS 26.1, iOS 18.7.2 and iPadOS 18.7.2, macOS Tahoe 26.1, visionOS 26.1, tvOS 26.1, macOS Sonoma 14.8.2, macOS Sequoia 15.7.2, iOS 26.1 and iPadOS 26.1. A malicious application may be able to cause unexpected system termination or write kernel memory. |
| **Root Cause** | Use vendor advisories and patch notes for authoritative technical details. |
| **Exploitation Prerequisite** | Affected version is reachable through an exploitable path and remains unpatched. |
| **Exploit Path** | Attacker leverages public PoC or observed exploit chain for intrusion. |
| **Affected Products** | apple/ipados, apple/iphone_os, apple/macos, apple/tvos, apple/visionos |
| **Risk Score** | 7.1 (HIGH) |
| **Exploited in the wild** | Listed in CISA KEV |
| **KEV remediation due date** | 2026-04-03 |
| **Mitigation** | Apply vendor patches immediately, reduce internet exposure, harden WAF/ACL controls, and enable anomaly detection. Since active exploitation is observed, patch high-risk assets within 24 hours. |
| **Source** | https://www.cisa.gov/known-exploited-vulnerabilities-catalog |
| **Source** | https://nvd.nist.gov/vuln/detail/CVE-2025-43520 |

## CVE-2025-31277

| | |
|---|---|
| **CVE Title** | CVE-2025-31277 \| apple/safari \| Unknown Type |
| **CVE Description** | The issue was addressed with improved memory handling. This issue is fixed in Safari 18.6, watchOS 11.6, visionOS 2.6, iOS 18.6 and iPadOS 18.6, macOS Sequoia 15.6, tvOS 18.6. Processing maliciously crafted web content may lead to memory corruption. |
| **Root Cause** | Use vendor advisories and patch notes for authoritative technical details. |
| **Exploitation Prerequisite** | Affected version is reachable through an exploitable path and remains unpatched. |
| **Exploit Path** | Attacker leverages public PoC or observed exploit chain for intrusion. |
| **Affected Products** | apple/safari, apple/ipados, apple/iphone_os, apple/macos, apple/tvos |
| **Risk Score** | 8.8 (HIGH) |
| **Exploited in the wild** | Listed in CISA KEV |
| **KEV remediation due date** | 2026-04-03 |
| **Mitigation** | Apply vendor patches immediately, reduce internet exposure, harden WAF/ACL controls, and enable anomaly detection. Since active exploitation is observed, patch high-risk assets within 24 hours. |
| **Source** | https://www.cisa.gov/known-exploited-vulnerabilities-catalog |
| **Source** | https://nvd.nist.gov/vuln/detail/CVE-2025-31277 |

## CVE-2026-20131

| | |
|---|---|
| **CVE Title** | CVE-2026-20131 \| cisco/secure_firewall_management_center \| Deserialization |
| **CVE Description** | A vulnerability in the web-based management interface of Cisco Secure Firewall Management Center (FMC) Software could allow an unauthenticated, remote attacker to execute arbitrary Java code as root on an affected device. |
| **Root Cause** | Use vendor advisories and patch notes for authoritative technical details. |
| **Exploitation Prerequisite** | Affected version is reachable through an exploitable path and remains unpatched. |
| **Exploit Path** | Attacker leverages public PoC or observed exploit chain for intrusion. |
| **Affected Products** | cisco/secure_firewall_management_center |
| **Risk Score** | 10.0 (CRITICAL) |
| **Exploited in the wild** | Listed in CISA KEV |
| **KEV remediation due date** | 2026-03-22 |
| **Mitigation** | Apply vendor patches immediately, reduce internet exposure, harden WAF/ACL controls, and enable anomaly detection. Since active exploitation is observed, patch high-risk assets within 24 hours. |
| **Source** | https://www.cisa.gov/known-exploited-vulnerabilities-catalog |
| **Source** | https://nvd.nist.gov/vuln/detail/CVE-2026-20131 |

## CVE-2025-66376

| | |
|---|---|
| **CVE Title** | CVE-2025-66376 \| synacor/zimbra_collaboration_suite \| XSS |
| **CVE Description** | Zimbra Collaboration (ZCS) 10 before 10.0.18 and 10.1 before 10.1.13 allows Classic UI stored XSS via Cascading Style Sheets (CSS) @import directives in an HTML e-mail message. |
| **Root Cause** | Use vendor advisories and patch notes for authoritative technical details. |
| **Exploitation Prerequisite** | Affected version is reachable through an exploitable path and remains unpatched. |
| **Exploit Path** | Attacker leverages public PoC or observed exploit chain for intrusion. |
| **Affected Products** | synacor/zimbra_collaboration_suite |
| **Risk Score** | 7.2 (HIGH) |
| **Exploited in the wild** | Listed in CISA KEV |
| **KEV remediation due date** | 2026-04-01 |
| **Mitigation** | Apply vendor patches immediately, reduce internet exposure, harden WAF/ACL controls, and enable anomaly detection. Since active exploitation is observed, patch high-risk assets within 24 hours. |
| **Source** | https://www.cisa.gov/known-exploited-vulnerabilities-catalog |
| **Source** | https://nvd.nist.gov/vuln/detail/CVE-2025-66376 |

### CVE-2026-20963

| | |
|---|---|
| **CVE Title** | CVE-2026-20963 \| microsoft/sharepoint_server \| Deserialization |
| **CVE Description** | Deserialization of untrusted data in Microsoft Office SharePoint allows an authorized attacker to execute code over a network. |
| **Root Cause** | Use vendor advisories and patch notes for authoritative technical details. |
| **Exploitation Prerequisite** | Affected version is reachable through an exploitable path and remains unpatched. |
| **Exploit Path** | Attacker leverages public PoC or observed exploit chain for intrusion. |
| **Affected Products** | microsoft/sharepoint_server |
| **Risk Score** | 8.8 (HIGH) |
| **Exploited in the wild** | Listed in CISA KEV |
| **KEV remediation due date** | 2026-03-21 |
| **Mitigation** | Apply vendor patches immediately, reduce internet exposure, harden WAF/ACL controls, and enable anomaly detection. Since active exploitation is observed, patch high-risk assets within 24 hours. |
| **Source** | https://www.cisa.gov/known-exploited-vulnerabilities-catalog |
| **Source** | https://nvd.nist.gov/vuln/detail/CVE-2026-20963 |

## 🧪 Report A2: Newly Published CVEs (NVD, last 7 days)

## CVE-2013-20005

| | |
|---|---|
| **CVE Title** | CVE-2013-20005 \| 待核實 \| Unknown Type |
| **CVE Description** | Qool CMS 2.0 RC2 contains a cross-site request forgery vulnerability that allows attackers to perform administrative actions by tricking logged-in users into visiting malicious web pages. Attackers can forge POST requests to the /admin/adduser endpoint with parameters like username, password, email, and level to create root-level user accounts without user consent. |
| **Affected Products** | 待核實 |
| **Risk Score** | 5.3 (MEDIUM) |
| **Source** | https://nvd.nist.gov/vuln/detail/CVE-2013-20005 |

## CVE-2013-20006

| | |
|---|---|
| **CVE Title** | CVE-2013-20006 \| 待核實 \| XSS |
| **CVE Description** | Qool CMS contains multiple persistent cross-site scripting vulnerabilities in several administrative scripts where POST parameters are not properly sanitized before being stored and returned to users. Attackers can inject malicious JavaScript code through parameters like 'title', 'name', 'email', 'username', 'link', and 'task' in endpoints such as addnewtyp... |
| **Affected Products** | 待核實 |
| **Risk Score** | 7.5 (HIGH) |
| **Source** | https://nvd.nist.gov/vuln/detail/CVE-2013-20006 |

## CVE-2015-20113

| | |
|---|---|
| **CVE Title** | CVE-2015-20113 \| nextclickventures/realtyscript \| XSS |
| **CVE Description** | Next Click Ventures RealtyScript 4.0.2 contains cross-site request forgery and persistent cross-site scripting vulnerabilities that allow attackers to perform administrative actions and inject malicious scripts. Attackers can craft malicious web pages that execute unauthorized actions when logged-in users visit them, or inject persistent scripts that execute in the application context. |
| **Affected Products** | nextclickventures/realtyscript |
| **Risk Score** | 5.3 (MEDIUM) |
| **Source** | https://nvd.nist.gov/vuln/detail/CVE-2015-20113 |

## CVE-2015-20114

| | |
|---|---|
| **CVE Title** | CVE-2015-20114 \| nextclickventures/realtyscript \| XSS |
| **CVE Description** | Next Click Ventures RealtyScript 4.0.2 contains a cross-site scripting vulnerability that allows attackers to execute arbitrary HTML and script code by injecting malicious input through multiple parameters that are not properly sanitized. Attackers can craft requests with injected script payloads in vulnerable parameters to execute code in users' browser sessions within the context of the affected application. |
| **Affected Products** | nextclickventures/realtyscript |
| **Risk Score** | 6.1 (MEDIUM) |
| **Source** | https://nvd.nist.gov/vuln/detail/CVE-2015-20114 |

### CVE-2015-20115

| | |
|---|---|
| **CVE Title** | CVE-2015-20115 \| nextclickventures/realtyscript \| Unknown Type |
| **CVE Description** | Next Click Ventures RealtyScript 4.0.2 fails to properly sanitize file uploads, allowing attackers to store malicious scripts through the file POST parameter in admin/tools.php. Attackers can upload files containing JavaScript code that executes in the context of admin/tools.php when accessed by other users. |
| **Affected Products** | nextclickventures/realtyscript |
| **Risk Score** | 7.2 (HIGH) |
| **Source** | https://nvd.nist.gov/vuln/detail/CVE-2015-20115 |

### CVE-2015-20116

| | |
|---|---|
| **CVE Title** | CVE-2015-20116 \| nextclickventures/realtyscript \| XSS |
| **CVE Description** | Next Click Ventures RealtyScript 4.0.2 fails to properly sanitize CSV file uploads, allowing attackers to inject malicious scripts through filename parameters in multipart form data. Attackers can upload files with XSS payloads in the filename field to execute arbitrary JavaScript in users' browsers when the file is processed or displayed. |
| **Affected Products** | nextclickventures/realtyscript |
| **Risk Score** | 6.1 (MEDIUM) |
| **Source** | https://nvd.nist.gov/vuln/detail/CVE-2015-20116 |

## Report B: Threat Intelligence News (last 7 days)

## Headline: CTI-REALM: A new benchmark for end-to-end detection rule generation with AI agents

| | |
|---|---|
| **Source** | Microsoft Security Blog |
| **Published** | Fri, 20 Mar 2026 16:19:00 +0000 |
| **Key Takeaway** | CTI-REALM: A new benchmark for end-to-end detection rule generation with AI agents |
| **Summary Engine** | extractive-rules |
| **Threat Actors** | Not explicitly stated |
| **Target** | technology/待核實 |
| **Technique** | 待核實 |
| **MITRE ATT&CK** | Unverified |
| **Related CVEs** | None |
| **Link** | https://www.microsoft.com/en-us/security/blog/2026/03/20/cti-realm-a-new-benchmark-for-end-to-end-detection-rule-generation-with-ai-agents/ |

## Headline: Secure agentic AI end-to-end

| | |
|---|---|
| **Source** | Microsoft Security Blog |
| **Published** | Fri, 20 Mar 2026 16:00:00 +0000 |
| **Key Takeaway** | Secure agentic AI end-to-end |
| **Summary Engine** | extractive-rules |
| **Threat Actors** | Not explicitly stated |
| **Target** | technology/待核實 |
| **Technique** | 待核實 |
| **MITRE ATT&CK** | Unverified |
| **Related CVEs** | None |
| **Link** | https://www.microsoft.com/en-us/security/blog/2026/03/20/secure-agentic-ai-end-to-end/ |

## Headline: CISA Issues Updated RESURGE Malware Analysis Highlighting a Stealthy but Active Threat

| | |
|---|---|
| **Source** | CISA News |
| **Published** | Thu, 26 Feb 26 12:00:00 +0000 |
| **Key Takeaway** | CISA Issues Updated RESURGE Malware Analysis Highlighting a Stealthy but Active Threat |
| **Summary Engine** | extractive-rules |
| **Threat Actors** | Not explicitly stated |
| **Target** | unknown-target |
| **Technique** | Malware Deployment |
| **MITRE ATT&CK** | Unverified |
| **Related CVEs** | None |
| **Link** | https://www.cisa.gov/news-events/news/cisa-issues-updated-resurge-malware-analysis-highlighting-stealthy-active-threat |

## Headline: Immediate Action Required: CISA Issues Emergency Directive to Secure Cisco SD-WAN Systems

| | |
|---|---|
| **Source** | CISA News |
| **Published** | Wed, 25 Feb 26 12:00:00 +0000 |
| **Key Takeaway** | Immediate Action Required: CISA Issues Emergency Directive to Secure Cisco SD-WAN Systems |
| **Summary Engine** | extractive-rules |
| **Threat Actors** | Not explicitly stated |
| **Target** | unknown-target |
| **Technique** | 待核實 |
| **MITRE ATT&CK** | Unverified |
| **Related CVEs** | None |
| **Link** | https://www.cisa.gov/news-events/news/immediate-action-required-cisa-issues-emergency-directive-secure-cisco-sd-wan-systems |

## Headline: The Proliferation of DarkSword: iOS Exploit Chain Adopted by Multiple Threat Actors

| | |
|---|---|
| **Source** | Mandiant Blog |
| **Published** | Wed, 18 Mar 2026 14:00:00 +0000 |
| **Key Takeaway** | Introduction Google Threat Intelligence Group (GTIG) has identified a new iOS full-chain exploit that leveraged multiple zero-day vulnerabilities to fully compromise devices. Based on toolmarks in recovered payloads, we believe the exploit chain to be called DarkSword. Recommendation: prioritize vulnerable-version inventory, accelerate patching, and monitor anomalous logins/lateral movement. |
| **Summary Engine** | extractive-rules |
| **Threat Actors** | Sandworm |
| **Target** | government/uk |
| **Technique** | Malware Deployment |
| **MITRE ATT&CK** | Unverified |
| **Related CVEs** | CVE-2025-14174, CVE-2025-31277, CVE-2025-43510, CVE-2025-43520, CVE-2025-43529, CVE-2026-20700 |
| **Link** | https://cloud.google.com/blog/topics/threat-intelligence/darksword-ios-exploit-chain/ |

## Headline: Ransomware Under Pressure: Tactics, Techniques, and Procedures in a Shifting Threat Landscape

| | |
|---|---|
| **Source** | Mandiant Blog |
| **Published** | Mon, 16 Mar 2026 14:00:00 +0000 |
| **Key Takeaway** | Written by: Bavi Sadayappan, Zach Riddle, Ioana Teaca, Kimberly Goody, Genevieve Stark Introduction Since 2018, when many financially motivated threat actors began shifting their monetization strategy to post-compromise ransomware deployments, ransomware has become one of the most pervasive threats Recommendation: prioritize vulnerable-version inventory, accelerate patching, and monitor anomalous logins/lateral move... |
| **Summary Engine** | extractive-rules |
| **Threat Actors** | ALPHV, Akira, Cl0p, LockBit |
| **Target** | government/europe |
| **Technique** | Social Engineering |
| **MITRE ATT&CK** | Unverified |
| **Related CVEs** | CVE-2019-6693, CVE-2021-27877, CVE-2021-27878, CVE-2021-40539, CVE-2023-4966, CVE-2024-21762, CVE-2024-3400, CVE-2024-37085, CVE-2024-40766, CVE-2024-55591, CVE-2025-31161, CVE-2025-31324, CVE-2025-53770, CVE-2025-53771, CVE-2025-61882, CVE-2025-8088 |
| **Link** | https://cloud.google.com/blog/topics/threat-intelligence/ransomware-ttps-shifting-threat-landscape/ |

## Headline: You have to invite them in

| | |
|---|---|
| **Source** | Cisco Talos Blog |
| **Published** | Thu, 19 Mar 2026 18:00:34 GMT |
| **Key Takeaway** | You have to invite them in Blog Intelligence Center Intelligence Center BACK Intelligence Search Email & Spam Trends Vulnerability Research Vulnerability Research BACK Vulnerability Reports Microsoft Advisories Incident Response Incident Response BACK Reactive Services Proactive Services Emergency S Recommendation: prioritize vulnerable-version inventory, accelerate patching, and monitor anomalous logins/lateral... |
| **Summary Engine** | extractive-rules |
| **Threat Actors** | Not explicitly stated |
| **Target** | unknown-target |
| **Technique** | 待核實 |
| **MITRE ATT&CK** | Unverified |
| **Related CVEs** | None |
| **Link** | https://blog.talosintelligence.com/you-have-to-invite-them-in/ |

## Headline: Everyday tools, extraordinary crimes: the ransomware exfiltration playbook

| | |
|---|---|
| **Source** | Cisco Talos Blog |
| **Published** | Thu, 19 Mar 2026 10:00:38 GMT |
| **Key Takeaway** | Everyday tools, extraordinary crimes: the ransomware exfiltration playbook Blog Intelligence Center Intelligence Center BACK Intelligence Search Email & Spam Trends Vulnerability Research Vulnerability Research BACK Vulnerability Reports Microsoft Advisories Incident Response Incident Response BACK Recommendation: prioritize vulnerable-version inventory, accelerate patching, and monitor anomalous logins/lateral... |
| **Summary Engine** | extractive-rules |
| **Threat Actors** | Not explicitly stated |
| **Target** | cloud/待核實 |
| **Technique** | Ransomware |
| **MITRE ATT&CK** | Unverified |
| **Related CVEs** | None |
| **Link** | https://blog.talosintelligence.com/everyday-tools-extraordinary-crimes-the-ransomware-exfiltration-playbook/ |

## Headline: FBI Warns Russian Hackers Target Signal, WhatsApp in Mass Phishing Attacks

| | |
|---|---|
| **Source** | The Hacker News |
| **Published** | Sat, 21 Mar 2026 18:47:00 +0530 |
| **Key Takeaway** | Threat actors affiliated with Russian Intelligence Services are conducting phishing campaigns to compromise commercial messaging applications (CMAs) like WhatsApp and Signal to seize control of accounts belonging to individuals with high intelligence value, the U.S. "The campaign FBI Warns Russian H Recommendation: prioritize vulnerable-version inventory, accelerate patching, and monitor anomalous logins/latera... |
| **Summary Engine** | extractive-rules |
| **Threat Actors** | Not explicitly stated |
| **Target** | unknown-target |
| **Technique** | Phishing |
| **MITRE ATT&CK** | Unverified |
| **Related CVEs** | None |
| **Link** | https://thehackernews.com/2026/03/fbi-warns-russian-hackers-target-signal.html |

## Headline: Oracle Patches Critical CVE-2026-21992 Enabling Unauthenticated RCE in Identity Manager

| | |
|---|---|
| **Source** | The Hacker News |
| **Published** | Sat, 21 Mar 2026 15:54:00 +0530 |
| **Key Takeaway** | Oracle has released security updates to address a critical security flaw impacting Identity Manager and Web Services Manager that could be exploited to achieve remote code execution. The vulnerability, tracked as CVE-2026-21992, carries a CVSS score of 9.8 out of a maximum of 10.0. Recommendation: prioritize vulnerable-version inventory, accelerate patching, and monitor anomalous logins/lateral movement. |
| **Summary Engine** | extractive-rules |
| **Threat Actors** | Not explicitly stated |
| **Target** | ot/待核實 |
| **Technique** | Exploit Chain |
| **MITRE ATT&CK** | Unverified |
| **Related CVEs** | CVE-2026-21992 |
| **Link** | https://thehackernews.com/2026/03/oracle-patches-critical-cve-2026-21992.html |

## Headline: Critical Quest KACE Vulnerability Potentially Exploited in Attacks

| | |
|---|---|
| **Source** | SecurityWeek |
| **Published** | Sat, 21 Mar 2026 11:00:00 +0000 |
| **Key Takeaway** | The vulnerability is tracked as CVE-2025-32975 and it may have been exploited in attacks against the education sector. The post Critical Quest KACE Vulnerability Potentially Exploited in Attacks appeared first on SecurityWeek . Recommendation: prioritize vulnerable-version inventory, accelerate patching, and monitor anomalous logins/lateral movement. |
| **Summary Engine** | extractive-rules |
| **Threat Actors** | Not explicitly stated |
| **Target** | education/待核實 |
| **Technique** | Exploit Chain |
| **MITRE ATT&CK** | Unverified |
| **Related CVEs** | CVE-2025-32975 |
| **Link** | https://www.securityweek.com/critical-quest-kace-vulnerability-potentially-exploited-in-attacks/ |

## Headline: In Other News: New Android Safeguards, Operation Alice, UK Toughens Cyber Reporting

| | |
|---|---|
| **Source** | SecurityWeek |
| **Published** | Fri, 20 Mar 2026 15:57:30 +0000 |
| **Key Takeaway** | Other noteworthy stories that might have slipped under the radar: vulnerabilities found in KVM devices, Claudy Day Claude vulnerabilities, The Gentlemen ransomware group. In Other News: New Android Safeguards, Operation Alice, UK Toughens Cyber Reporting - SecurityWeek SECURITYWEEK NETWORK: Cybersec Recommendation: prioritize vulnerable-version inventory, accelerate patching, and monitor anomalous logins/lateral mov... |
| **Summary Engine** | extractive-rules |
| **Threat Actors** | Not explicitly stated |
| **Target** | ot/uk |
| **Technique** | Ransomware |
| **MITRE ATT&CK** | Unverified |
| **Related CVEs** | None |
| **Link** | https://www.securityweek.com/in-other-news-new-android-safeguards-operation-alice-uk-toughens-cyber-reporting/ |

## 📚 Sources (official/authoritative first)

**https://www.cisa.gov/known-exploited-vulnerabilities-catalog**

**https://nvd.nist.gov/**

**https://www.cve.org/**

https://attack.mitre.org/

https://www.microsoft.com/en-us/security/blog/

https://www.cisa.gov/news-events/cybersecurity-advisories

https://www.mandiant.com/resources

https://blog.talosintelligence.com/