🛡️ Weekly IT Security Brief (Official-source-first) | 2026-03-29 06:01

Formatted for readability · Auto-generated

📌 Weekly Summary

- Priority snapshot: 3 KEV-listed vulnerabilities are actively exploited in the wild (top 8 shown in this brief).
- Urgent patch focus: CVE-2025-53521(2026-03-30), CVE-2026-33634(2026-04-09), CVE-2026-33017(2026-04-08). Prioritize internet-facing and privileged systems first.
- Threat trend #1: How Microsoft Defender protects high-value assets in real-world attack scenarios. How Microsoft Defender protects high-value assets in real-world attack scenarios
- Threat trend #2: Identity security is the new pressure point for modern cyberattacks. Identity security is the new pressure point for modern cyberattacks
- 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-2025-53521

CVE Title	CVE-2025-53521 | f5/big-ip_access_policy_manager | Remote Code Execution
CVE Description	When a BIG-IP APM access policy is configured on a virtual server, specific malicious traffic can lead to Remote Code Execution (RCE).
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	f5/big-ip_access_policy_manager, f5/big-ip_advanced_firewall_manager, f5/big-ip_advanced_web_application_firewall, f5/big-ip_analytics, f5/big-ip_application_acceleration_manager
Risk Score	9.8 (CRITICAL)
Exploited in the wild	Listed in CISA KEV
KEV remediation due date	2026-03-30
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-2025-53521

CVE-2026-33634

CVE Title	CVE-2026-33634 | aquasec/setup-trivy | Unknown Type
CVE Description	Trivy is a security scanner. On March 19, 2026, a threat actor used compromised credentials to publish a malicious Trivy v0.69.4 release, force-push 76 of 77 version tags in `aquasecurity/trivy-action` to credential-stealing malware, and replace all 7 tags in `aquasecurity/setup-trivy` with malicious commits. This incident is a continuation of the supply chain attack that began in late February 2026. Following the i...
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	aquasec/setup-trivy, aquasec/trivy, aquasec/trivy_action, litellm/litellm
Risk Score	8.8 (HIGH)
Exploited in the wild	Listed in CISA KEV
KEV remediation due date	2026-04-09
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-2026-33634

CVE-2026-33017

CVE Title	CVE-2026-33017 | langflow/langflow | Remote Code Execution
CVE Description	Langflow is a tool for building and deploying AI-powered agents and workflows. In versions prior to 1.9.0, the POST /api/v1/build_public_tmp/{flow_id}/flow endpoint allows building public flows without requiring authentication. When the optional data parameter is supplied, the endpoint uses attacker-controlled flow data (containing arbitrary Python code in node definitions) instead of the stored flow data from the d...
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	langflow/langflow
Risk Score	9.8 (CRITICAL)
Exploited in the wild	Listed in CISA KEV
KEV remediation due date	2026-04-08
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-2026-33017

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

CVE-2026-4528

CVE Title	CVE-2026-4528 | 待核實 | SSRF
CVE Description	A vulnerability was determined in trueleaf ApiFlow 0.9.7. The impacted element is the function validateUrlSecurity of the file packages/server/src/service/proxy/http_proxy.service.ts of the component URL Validation Handler. This manipulation causes server-side request forgery. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized.
Affected Products	待核實
Risk Score	7.3 (HIGH)
Source	https://nvd.nist.gov/vuln/detail/CVE-2026-4528

CVE-2026-3629

CVE Title	CVE-2026-3629 | 待核實 | Privilege Escalation
CVE Description	The Import and export users and customers plugin for WordPress is vulnerable to privilege escalation in all versions up to, and including, 1.29.7. This is due to the 'save_extra_user_profile_fields' function not properly restricting which user meta keys can be updated via profile fields. The 'get_restricted_fields' method does not include sensitive meta keys such as 'wp_capabilities'. T...
Affected Products	待核實
Risk Score	8.1 (HIGH)
Source	https://nvd.nist.gov/vuln/detail/CVE-2026-3629

CVE-2026-4529

CVE Title	CVE-2026-4529 | 待核實 | Buffer Overflow
CVE Description	A vulnerability was identified in D-Link DHP-1320 1.00WWB04. This affects the function redirect_count_down_page of the component SOAP Handler. Such manipulation leads to stack-based buffer overflow. The attack can be executed remotely. The exploit is publicly available and might be used. This vulnerability only affects products that are no longer supported by the maintainer.
Affected Products	待核實
Risk Score	8.8 (HIGH)
Source	https://nvd.nist.gov/vuln/detail/CVE-2026-4529

CVE-2026-4530

CVE Title	CVE-2026-4530 | 待核實 | SQL Injection
CVE Description	A security flaw has been discovered in apconw Aix-DB up to 1.2.3. This impacts an unknown function of the file agent/text2sql/rag/terminology_retriever.py. Performing a manipulation of the argument Description results in sql injection. The attack requires a local approach. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond...
Affected Products	待核實
Risk Score	5.3 (MEDIUM)
Source	https://nvd.nist.gov/vuln/detail/CVE-2026-4530

CVE-2019-25583

CVE Title	CVE-2019-25583 | raimersoft/rarmaradio | Unknown Type
CVE Description	RarmaRadio 2.72.3 contains a denial of service vulnerability in the Username field that allows local attackers to crash the application by submitting excessively long input. Attackers can paste a buffer of 5000 bytes into the Username field via Settings > Network to trigger an application crash.
Affected Products	raimersoft/rarmaradio
Risk Score	6.2 (MEDIUM)
Source	https://nvd.nist.gov/vuln/detail/CVE-2019-25583

CVE-2019-25584

CVE Title	CVE-2019-25584 | raimersoft/rarmaradio | Buffer Overflow
CVE Description	RarmaRadio 2.72.3 contains a buffer overflow vulnerability in the Server field of the Network settings that allows local attackers to crash the application by supplying an excessively long string. Attackers can paste a malicious payload exceeding 4000 bytes into the Server field via the Settings menu to trigger an application crash.
Affected Products	raimersoft/rarmaradio
Risk Score	6.2 (MEDIUM)
Source	https://nvd.nist.gov/vuln/detail/CVE-2019-25584

Report B: Threat Intelligence News (last 7 days)

Headline: How Microsoft Defender protects high-value assets in real-world attack scenarios

Source	Microsoft Security Blog
Published	Fri, 27 Mar 2026 19:53:53 +0000
Key Takeaway	How Microsoft Defender protects high-value assets in real-world attack scenarios
Summary Engine	extractive-rules
Threat Actors	Not explicitly stated
Target	defense/待核實
Technique	待核實
MITRE ATT&CK	Unverified
Related CVEs	None
Link	https://www.microsoft.com/en-us/security/blog/2026/03/27/microsoft-defender-protects-high-value-assets/

Headline: Identity security is the new pressure point for modern cyberattacks

Source	Microsoft Security Blog
Published	Wed, 25 Mar 2026 16:00:00 +0000
Key Takeaway	Identity security is the new pressure point for modern cyberattacks
Summary Engine	extractive-rules
Threat Actors	Not explicitly stated
Target	ot/待核實
Technique	待核實
MITRE ATT&CK	Unverified
Related CVEs	None
Link	https://www.microsoft.com/en-us/security/blog/2026/03/25/identity-security-is-the-new-pressure-point-for-modern-cyberattacks/

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: M-Trends 2026: Data, Insights, and Strategies From the Frontlines

Source	Mandiant Blog
Published	Mon, 23 Mar 2026 14:00:00 +0000
Key Takeaway	Every year, the cyber threat landscape forces defenders to adapt to evolving adversary tactics, techniques, and procedures (TTPs). Grounded in over 500,000 hours of frontline incident investigations conducted by Mandiant globally in 2025, this report provides a definitive look at the TTPs actively b Recommendation: prioritize vulnerable-version inventory, accelerate patching, and monitor anomalous logins/lateral mov...
Summary Engine	extractive-rules
Threat Actors	Akira
Target	defense/global
Technique	Social Engineering
MITRE ATT&CK	Unverified
Related CVEs	None
Link	https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2026/

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: TP-Link, Canva, HikVision vulnerabilities

Source	Cisco Talos Blog
Published	Thu, 26 Mar 2026 18:34:26 GMT
Key Takeaway	Cisco Talos' Vulnerability Discovery & Research team recently disclosed a vulnerability in HikVision, as well as 10 in TP-Link, and 19 in Canva. The vulnerabilities mentioned in this blog post have been patched by their respective vendors, all in adherence to Cisco's third-party vulnerability disclo 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/tp-link-canva-hikvision-vulnerabilities/

Headline: A puppet made me cry and all I got was this t-shirt

Source	Cisco Talos Blog
Published	Thu, 26 Mar 2026 18:00:44 GMT
Key Takeaway	A puppet made me cry and all I got was this t-shirt 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 Proac Recommendation: prioritize vulnerable-version inventory, accelerate patching, and monitor anomalous logins/lateral...
Summary Engine	extractive-rules
Threat Actors	Not explicitly stated
Target	ot/待核實
Technique	待核實
MITRE ATT&CK	Unverified
Related CVEs	None
Link	https://blog.talosintelligence.com/a-puppet-made-me-cry-and-all-i-got-was-this-t-shirt/

Headline: Iran-Linked Hackers Breach FBI Director’s Personal Email, Hit Stryker With Wiper Attack

Source	The Hacker News
Published	Sat, 28 Mar 2026 21:10:00 +0530
Key Takeaway	Handala Hack Team, which carried out the breach, said on its website that Patel "will now find his name among the list of successfully hacked victims." In a statement Iran-Linked Hackers Breach FBI Director’s Personal Email, Hit Stryker With Wiper Attack --> #1 Trusted Cybersecurity News Platform Fo Recommendation: prioritize vulnerable-version inventory, accelerate patching, and monitor anomalous login...
Summary Engine	extractive-rules
Threat Actors	Not explicitly stated
Target	ot/待核實
Technique	待核實
MITRE ATT&CK	Unverified
Related CVEs	None
Link	https://thehackernews.com/2026/03/iran-linked-hackers-breach-fbi.html

Headline: Citrix NetScaler Under Active Recon for CVE-2026-3055 (CVSS 9.3) Memory Overread Bug

Source	The Hacker News
Published	Sat, 28 Mar 2026 14:41:00 +0530
Key Takeaway	The vulnerability, CVE-2026-3055 (CVSS score: 9.3), refers to a case of insufficient input validation leading to memory overread, which an attacker could exploit to leak potentially sensitive information. Per Citrix NetScaler Under Active Recon for CVE-2026-3055 (CVSS 9.3) Memory Overread Bug --> #1 Recommendation: prioritize vulnerable-version inventory, accelerate patching, and monitor anomalous logins/lateral...
Summary Engine	extractive-rules
Threat Actors	Not explicitly stated
Target	ot/待核實
Technique	Exploit Chain
MITRE ATT&CK	Unverified
Related CVEs	CVE-2026-3055
Link	https://thehackernews.com/2026/03/citrix-netscaler-under-active-recon-for.html

Headline: Cloudflare-Themed ClickFix Attack Drops Infiniti Stealer on Macs

Source	SecurityWeek
Published	Sat, 28 Mar 2026 10:30:00 +0000
Key Takeaway	The infection chain includes a fake CAPTCHA page, a Bash script, a Nuitka loader, and the Python-based infostealer. Cloudflare-Themed ClickFix Attack Drops Infiniti Stealer on Macs - SecurityWeek SECURITYWEEK NETWORK: Cybersecurity News Webcasts Virtual Events ICS: ICS Cybersecurity Conference Malwa Recommendation: prioritize vulnerable-version inventory, accelerate patching, and monitor anomalous logins/lateral mov...
Summary Engine	extractive-rules
Threat Actors	Not explicitly stated
Target	cloud/待核實
Technique	待核實
MITRE ATT&CK	Unverified
Related CVEs	None
Link	https://www.securityweek.com/cloudflare-themed-clickfix-attack-drops-infiniti-stealer-on-macs/

Headline: Pro-Iranian Hacking Group Claims Credit for Hack of FBI Director Kash Patel’s Personal Account

Source	SecurityWeek
Published	Fri, 27 Mar 2026 16:42:22 +0000
Key Takeaway	Pro-Iranian Hacking Group Claims Credit for Hack of FBI Director Kash Patel’s Personal Account - SecurityWeek SECURITYWEEK NETWORK: Cybersecurity News Webcasts Virtual Events ICS: ICS Cybersecurity Conference Malware & Threats Cyberwarfare Cybercrime Data Breaches Fraud & Identity Theft Nation-State Recommendation: prioritize vulnerable-version inventory, accelerate patching, and monitor anomalous logins/lat...
Summary Engine	extractive-rules
Threat Actors	Not explicitly stated
Target	ot/待核實
Technique	待核實
MITRE ATT&CK	Unverified
Related CVEs	None
Link	https://www.securityweek.com/pro-iranian-hacking-group-claims-credit-for-hack-of-fbi-director-kash-patels-personal-account/

📚 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/