🛡️ Weekly IT Security Brief (Official-source-first) | 2026-03-16 16:01

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-2026-3910(2026-03-27), CVE-2026-3909(2026-03-27), CVE-2025-68613(2026-03-25). Prioritize internet-facing and privileged systems first.
- Threat trend #1: Storm-2561 uses SEO poisoning to distribute fake VPN clients for credential theft. Storm-2561 uses SEO poisoning to distribute fake VPN clients for credential theft
- Threat trend #2: From transparency to action: What the latest Microsoft email security benchmark reveals. From transparency to action: What the latest Microsoft email security benchmark reveals
- 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-2026-3910

CVE Title	CVE-2026-3910 | google/chrome | Unknown Type
CVE Description	Inappropriate implementation in V8 in Google Chrome prior to 146.0.7680.75 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)
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	google/chrome, apple/macos, linux/linux_kernel, microsoft/windows
Risk Score	8.8 (HIGH)
Exploited in the wild	Listed in CISA KEV
KEV remediation due date	2026-03-27
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-2026-3910

CVE-2026-3909

CVE Title	CVE-2026-3909 | google/chrome | Unknown Type
CVE Description	Out of bounds write in Skia in Google Chrome prior to 146.0.7680.75 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High)
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	google/chrome, apple/macos, linux/linux_kernel, microsoft/windows
Risk Score	8.8 (HIGH)
Exploited in the wild	Listed in CISA KEV
KEV remediation due date	2026-03-27
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-2026-3909

CVE-2025-68613

CVE Title	CVE-2025-68613 | n8n/n8n | Remote Code Execution
CVE Description	n8n is an open source workflow automation platform. Versions starting with 0.211.0 and prior to 1.120.4, 1.121.1, and 1.122.0 contain a critical Remote Code Execution (RCE) vulnerability in their workflow expression evaluation system. Under certain conditions, expressions supplied by authenticated users during workflow configuration may be evaluated in an execution context that is not sufficiently isolated from the...
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	n8n/n8n
Risk Score	9.9 (CRITICAL)
Exploited in the wild	Listed in CISA KEV
KEV remediation due date	2026-03-25
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-2025-68613

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

CVE-2026-3808

CVE Title	CVE-2026-3808 | tenda/fh1202_firmware | Buffer Overflow
CVE Description	A vulnerability was detected in Tenda FH1202 1.2.0.14(408). The affected element is the function formWebTypeLibrary of the file /goform/webtypelibrary. Performing a manipulation of the argument webSiteId results in stack-based buffer overflow. The attack may be initiated remotely. The exploit is now public and may be used.
Affected Products	tenda/fh1202_firmware, tenda/fh1202
Risk Score	8.8 (HIGH)
Source	https://nvd.nist.gov/vuln/detail/CVE-2026-3808

CVE-2026-3809

CVE Title	CVE-2026-3809 | tenda/fh1202_firmware | Buffer Overflow
CVE Description	A flaw has been found in Tenda FH1202 1.2.0.14(408). The impacted element is the function fromNatStaticSetting of the file /goform/NatSaticSetting. Executing a manipulation of the argument page can lead to stack-based buffer overflow. The attack may be launched remotely. The exploit has been published and may be used.
Affected Products	tenda/fh1202_firmware, tenda/fh1202
Risk Score	8.8 (HIGH)
Source	https://nvd.nist.gov/vuln/detail/CVE-2026-3809

CVE-2026-3810

CVE Title	CVE-2026-3810 | tenda/fh1202_firmware | Buffer Overflow
CVE Description	A vulnerability has been found in Tenda FH1202 1.2.0.14(408). This affects the function fromDhcpListClient of the file /goform/DhcpListClient. The manipulation of the argument page leads to stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used.
Affected Products	tenda/fh1202_firmware, tenda/fh1202
Risk Score	8.8 (HIGH)
Source	https://nvd.nist.gov/vuln/detail/CVE-2026-3810

CVE-2025-41754

CVE Title	CVE-2025-41754 | mbs-solutions/universal_bacnet_router_firmware | Unknown Type
CVE Description	A low-privileged remote attacker can exploit the ubr-editfile method in wwwubr.cgi, an undocumented and unused API endpoint to read arbitrary files on the system.
Affected Products	mbs-solutions/universal_bacnet_router_firmware, mbs-solutions/ubr-01_mk_ii, mbs-solutions/ubr-02, mbs-solutions/ubr-lon
Risk Score	6.5 (MEDIUM)
Source	https://nvd.nist.gov/vuln/detail/CVE-2025-41754

CVE-2025-41755

CVE Title	CVE-2025-41755 | mbs-solutions/universal_bacnet_router_firmware | Unknown Type
CVE Description	A low-privileged remote attacker can exploit the ubr-logread method in wwwubr.cgi to read arbitrary files on the system. The endpoint accepts a parameter specifying the log file to open (e.g., /tmp/weblog{some_number}), but this parameter is not properly validated, allowing an attacker to modify it to reference any file and retrieve its contents.
Affected Products	mbs-solutions/universal_bacnet_router_firmware, mbs-solutions/ubr-01_mk_ii, mbs-solutions/ubr-02, mbs-solutions/ubr-lon
Risk Score	6.5 (MEDIUM)
Source	https://nvd.nist.gov/vuln/detail/CVE-2025-41755

CVE-2025-41756

CVE Title	CVE-2025-41756 | mbs-solutions/universal_bacnet_router_firmware | Unknown Type
CVE Description	A low-privileged remote attacker can exploit the ubr-editfile method in wwwubr.cgi, an undocumented and unused API endpoint to write arbitrary files on the system.
Affected Products	mbs-solutions/universal_bacnet_router_firmware, mbs-solutions/ubr-01_mk_ii, mbs-solutions/ubr-02, mbs-solutions/ubr-lon
Risk Score	8.1 (HIGH)
Source	https://nvd.nist.gov/vuln/detail/CVE-2025-41756

Report B: Threat Intelligence News (last 7 days)

Headline: Storm-2561 uses SEO poisoning to distribute fake VPN clients for credential theft

Source	Microsoft Security Blog
Published	Thu, 12 Mar 2026 17:00:00 +0000
Key Takeaway	Storm-2561 uses SEO poisoning to distribute fake VPN clients for credential theft
Summary Engine	extractive-rules
Threat Actors	Not explicitly stated
Target	ics/待核實
Technique	Credential Access
MITRE ATT&CK	Unverified
Related CVEs	None
Link	https://www.microsoft.com/en-us/security/blog/2026/03/12/storm-2561-uses-seo-poisoning-to-distribute-fake-vpn-clients-for-credential-theft/

Headline: From transparency to action: What the latest Microsoft email security benchmark reveals

Source	Microsoft Security Blog
Published	Thu, 12 Mar 2026 16:00:00 +0000
Key Takeaway	From transparency to action: What the latest Microsoft email security benchmark reveals
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/2026/03/12/from-transparency-to-action-what-the-latest-microsoft-email-security-benchmark-reveals/

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: This one’s for you, Mom

Source	Cisco Talos Blog
Published	Thu, 12 Mar 2026 18:00:01 GMT
Key Takeaway	This one’s for you, Mom 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 Supp 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/this-ones-for-you-mom/

Headline: DirectX, OpenFOAM, Libbiosig vulnerabilities

Source	Cisco Talos Blog
Published	Wed, 11 Mar 2026 20:26:57 GMT
Key Takeaway	Cisco Talos' Vulnerability Discovery & Research team recently disclosed vulnerabilities in the BioSig Project Libbiosig library and OpenCFD OpenFOAM, as well as an unpatched vulnerability in Microsoft DirectX. The vulnerabilities mentioned in this blog post have been patched by their respective vend Recommendation: prioritize vulnerable-version inventory, accelerate patching, and monitor anomalous logins/lateral...
Summary Engine	extractive-rules
Threat Actors	Not explicitly stated
Target	ios/待核實
Technique	待核實
MITRE ATT&CK	Unverified
Related CVEs	None
Link	https://blog.talosintelligence.com/directx-openfoam-libbiosig-vulnerabilities/

Headline: Android 17 Blocks Non-Accessibility Apps from Accessibility API to Prevent Malware Abuse

Source	The Hacker News
Published	Mon, 16 Mar 2026 11:13:00 +0530
Key Takeaway	Google is testing a new security feature as part of Android Advanced Protection Mode (AAPM) that prevents certain kinds of apps from using the accessibility services API. The change, incorporated in Android 17 Beta 2, was first reported by Android Authority last week. 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	Malware Deployment
MITRE ATT&CK	Unverified
Related CVEs	None
Link	https://thehackernews.com/2026/03/android-17-blocks-non-accessibility.html

Headline: OpenClaw AI Agent Flaws Could Enable Prompt Injection and Data Exfiltration

Source	The Hacker News
Published	Sat, 14 Mar 2026 21:47:00 +0530
Key Takeaway	China's National Computer Network Emergency Response Technical Team (CNCERT) has issued a warning about the security stemming from the use of OpenClaw (formerly Clawdbot and Moltbot), an open-source and self-hosted autonomous artificial intelligence (AI) agent. In a post shared on WeChat, CNCERT not Recommendation: prioritize vulnerable-version inventory, accelerate patching, and monitor anomalous logins/latera...
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/openclaw-ai-agent-flaws-could-enable.html

Headline: Loblaw Data Breach Impacts Customer Information

Source	SecurityWeek
Published	Sun, 15 Mar 2026 10:00:00 +0000
Key Takeaway	The post Loblaw Data Breach Impacts Customer Information appeared first on SecurityWeek . Loblaw Data Breach Impacts Customer Information - SecurityWeek SECURITYWEEK NETWORK: Cybersecurity News Webcasts Virtual Events ICS: ICS Cybersecurity Conference Malware & Threats Cyberwarfare Cybercrime Data B 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://www.securityweek.com/loblaw-data-breach-impacts-customer-information/

Headline: Critical HPE AOS-CX Vulnerability Allows Admin Password Resets

Source	SecurityWeek
Published	Sat, 14 Mar 2026 10:50:00 +0000
Key Takeaway	The vulnerability can be exploited remotely, without authentication, to circumvent existing authentication controls. The post Critical HPE AOS-CX Vulnerability Allows Admin Password Resets 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	ot/待核實
Technique	Exploit Chain
MITRE ATT&CK	Unverified
Related CVEs	None
Link	https://www.securityweek.com/critical-hpe-aos-cx-vulnerability-allows-admin-password-resets/

Headline: OpenAI says ChatGPT ads are not rolling out globally for now

Source	BleepingComputer
Published	Sun, 15 Mar 2026 19:13:28 -0400
Key Takeaway	OpenAI told BleepingComputer that ChatGPT ads on Free and Go plans are not yet rolling out outside the United States, even though some users noticed references to ads in the updated privacy policy. [...] OpenAI says ChatGPT ads are not rolling out globally for now News Featured Latest FBI seeks vict Recommendation: prioritize vulnerable-version inventory, accelerate patching, and monitor anomalous logins/lateral mov...
Summary Engine	extractive-rules
Threat Actors	Not explicitly stated
Target	ot/global
Technique	待核實
MITRE ATT&CK	Unverified
Related CVEs	None
Link	https://www.bleepingcomputer.com/news/artificial-intelligence/openai-says-chatgpt-ads-are-not-rolling-out-globally-for-now/

Headline: Betterleaks, a new open-source secrets scanner to replace Gitleaks

Source	BleepingComputer
Published	Sun, 15 Mar 2026 10:17:23 -0400
Key Takeaway	A new open-source tool called Betterleaks can scan directories, files, and git repositories and identify valid secrets using default or customized rules. [...] Betterleaks, a new open-source secrets scanner to replace Gitleaks News Featured Latest FBI seeks victims of Steam games used to spread malw Recommendation: prioritize vulnerable-version inventory, accelerate patching, and monitor anomalous logins/lateral mov...
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.bleepingcomputer.com/news/security/betterleaks-a-new-open-source-secrets-scanner-to-replace-gitleaks/

📚 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/

⚠️ Notes (fetch/read errors)

Mandiant Blog fetch failed: The read operation timed out