INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:39 UTC

February 2026 CVE Landscape: 13 Critical Vulnerabilities Mark 43% Drop from January

SECURITY ANALYSIS | CRITICAL

SCC Item ID	SCC-STY-2026-0018
Type	Security Analysis
Severity	CRITICAL
Affected Products	Multiple vendors and products (specific CVEs not extractable from available raw data)
Published	2026-03-12
Discovery Source	Rss

Executive Summary

February 2026 saw 13 critical-severity vulnerabilities identified by Recorded Future's Insikt Group, representing a 43% decline from January's critical vulnerability count, a notable but likely temporary reduction rather than a structural improvement in the threat landscape. For CISOs and board members, the headline drop should not signal reduced vigilance; patch cycles, vendor disclosure coordination, and seasonal reporting patterns all influence monthly volume, and a lower count of critical CVEs does not reduce the urgency of remediating the ones that exist. Security leaders should use this period of relatively lower volume to accelerate remediation of any outstanding critical findings and stress-test patch management processes before the next high-volume month. Note: This analysis is based on secondary reporting; for product-specific impact and detailed CVE IDs, obtain the full Recorded Future Insikt Group report directly.

Technical Analysis

Recorded Future's Insikt Group published its February 2026 CVE landscape assessment identifying 13 critical-severity vulnerabilities across the month, down sharply from January 2026 levels. The Zero Day Initiative's February 2026 Security Update Review provides corroborating coverage of the same disclosure period, particularly around Microsoft's February Patch Tuesday cycle, which historically anchors the monthly critical vulnerability count for enterprise environments.

The 43% month-over-month decline is significant in absolute terms but requires careful interpretation. Monthly CVE volume is shaped by vendor release cadences, coordinated disclosure timing, and researcher pipeline fluctuations rather than by underlying changes in attacker capability or intent. A compressed disclosure month does not mean fewer exploitable vulnerabilities in production environments, it means fewer were formally

catalogued and scored during the window.

The 13-critical and 43%-drop figures are attributed to Recorded Future's Insikt Group across multiple secondary sources but have not been directly verified against the original report. Confidence in these figures is medium pending direct review of the Recorded Future source publication. Specific CVE IDs, affected vendors, CVSS scores, and attack vectors cannot be confirmed from available secondary source material. Security teams should treat these figures as directionally accurate and obtain the full Insikt Group report for specific details before making remediation decisions.

For security operations, the practical implication of a lighter critical disclosure month is that patch prioritization becomes more tractable, fewer critical items competing for remediation resources. However, this window also coincides with a risk of complacency. Threat actors do not pause because disclosure volume drops; they exploit existing unpatched vulnerabilities regardless of what month they were assigned a CVE number. Vulnerability management programs that rely on monthly volume as a proxy for risk are structurally misaligned with how exploitation actually occurs.

Action Checklist

1. Preamble: Steps 1-2 require access to the full Recorded Future Insikt Group report. If that report is paywalled or inaccessible, proceed to Step 3 using publicly available vendor advisories and threat intelligence feeds.
2. Step 1: Obtain the full Insikt Group February 2026 CVE Landscape report from Recorded Future's blog (verify access and availability) and extract the specific CVE IDs, affected vendors, and CVSS scores before making prioritization decisions; do not rely on secondary summaries alone.
3. Step 2: Cross-reference the 13 critical CVEs against your asset inventory to determine which, if any, affect systems in your environment; prioritize any that are internet-facing or reside in critical network segments.
4. Step 3: If available, review the Zero Day Initiative's February 2026 Security Update Review for Patch Tuesday-specific context, particularly for Microsoft products and any vendor advisories released in the same window.
5. Step 4: Use the lower-volume month as an opportunity to close remediation gaps from January. A 43% drop in new critical disclosures is a relative reprieve, not a reduced threat posture; outstanding patches from prior months remain exploitable.
6. Step 5: Brief security leadership and relevant stakeholders with a framing note: monthly CVE volume fluctuates based on disclosure cadence, not attacker activity. Avoid presenting the drop as a risk reduction without qualifying that interpretation.
7. Step 6: Monitor for follow-on exploitation reporting, CISA KEV updates, vendor incident disclosures, and threat intelligence feeds to identify if any of the 13 critical CVEs move from disclosed to actively exploited status.

IR / Forensic Enrichment

Triage Priority	URGENT

Escalation Criteria	Escalate to CISO immediately if any of the 13 CVEs appear on CISA's Known Exploited Vulnerabilities list or if active exploitation is reported against systems in your environment; engage external IR firm if any unpatched critical systems are compromised within 7 days of PoC publication.
Recovery Notes	Post-containment: verify all patches have deployed successfully to prioritized systems using vulnerability scanner re-scan and compliance report; update CMDB with patch dates and validated application versions. Conduct a retrospective on any systems that were exploited prior to patching, capture forensic artifacts (Windows Event Logs 4688, 4624; process execution timeline; registry modifications; network connections), and brief incident response team on attack chain and detection gaps. Document lessons learned and update detection rules to catch similar exploitation attempts on future CVEs.
Forensic Artifacts	Windows Event Log: Security (Event IDs 4688 process creation, 4689 process termination, 4624 logon, 4625 logon failure) and System (Event ID 1000 application error) for process-level exploitation artifacts | Windows Registry: HKLM\Software\Microsoft\Windows\CurrentVersion\Run and HKCU\Software\Microsoft\Windows\CurrentVersion\Run for persistence mechanisms; HKLM\System\CurrentControlSet\Services for service-based implants | /var/log/auth.log, /var/log/syslog (Linux) and /var/log/messages (older systems) for process execution and privilege escalation attempts | Web application logs (access.log, error.log for Apache/Nginx, or IIS logs in C:\inetpub\logs\LogFiles) containing HTTP requests that match known CVE payloads | Network PCAP files from firewall/proxy appliances during suspected exploitation window, filtered for anomalous outbound connections, DNS queries, and known C2 domains

Per-Action IR Details

Preamble: Steps 1-2 require access to the full Recorded Future Insikt Group report. If that report is paywalled or inaccessible, proceed to Step 3 using publicly available vendor advisories and threat intelligence feeds.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparing for Incident Handling)

Controls: NIST IR-4(1) - Incident Handling Implementation, CIS 6.2 - Activate Incident Response Team

Compensating: Establish free TI feed subscriptions before analysis begins: enable CISA NVD API (nvd.nist.gov/api), configure Shodan/Censys API keys for asset discovery, subscribe to vendor security mailing lists (Microsoft, Adobe, Oracle), and set up Google Alerts for 'CVE + [vendor]' to catch public disclosures in real time.

Evidence: Before attempting access to paywalled reports, capture: (1) list of TI feeds already integrated into your environment (SIEM source list), (2) vendor advisory distribution list and response SLAs, (3) current asset inventory export (hostname, IP, OS, applications, last patch date).

Step 1: Obtain the full Insikt Group February 2026 CVE Landscape report from Recorded Future's blog (verify access and availability) and extract the specific CVE IDs, affected vendors, and CVSS scores before making prioritization decisions; do not rely on secondary summaries alone.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Intelligence Gathering and Analysis)

Controls: NIST SI-4(16) - Threat Intelligence Program, CIS 4.1 - Establish and Maintain a Data Inventory

Compensating: If Recorded Future report is paywalled: extract CVE list from NVD (nvd.nist.gov), filter by publication date (February 2026), CVSS ≥9.0, and status 'Active'. Cross-reference vendor IDs with official CVE JSON schema (curl https://nvd.nist.gov/feeds/json/cve/1.1/ to verify format). Document source URL, access timestamp, and data completeness in your ticket.

Evidence: Capture before analysis: (1) screenshot or PDF of the report access attempt with timestamp, (2) NVD export date and filtering criteria used, (3) vendor advisory URLs and publication dates for each CVE, (4) your current

vulnerability scanner output (Nessus, Qualys, or OpenVAS) showing which CVEs are already detected in your environment.

Step 2: Cross-reference the 13 critical CVEs against your asset inventory to determine which, if any, affect systems in your environment; prioritize any that are internet-facing or reside in critical network segments.

NIST Phase: Preparation

Reference: NIST 800-61r3 §3.2.1 (Triage and Early Containment)

Controls: NIST CM-8 - Information System Component Inventory, NIST RA-3 - Risk Assessment, CIS 2.1 - Address Unauthorized Software

Compensating: Use free asset discovery: run 'nmap -sV --script vuln' on your network CIDR ranges, export results to CSV (name, IP, port, service, version). Cross-match manually against the CVE list using a spreadsheet pivot or grep: 'grep -i "[product-version]" nmap_output.csv'. Tag rows with 'internet-facing' (if in DMZ or accessible from WAN) and 'critical-segment' (if supporting payment, auth, or data systems). Export prioritized list with justification.

Evidence: Before cross-referencing: (1) export current asset inventory (CMDB or spreadsheet) with hostname, IP, OS, installed applications, last patched date, network segment, and criticality tier, (2) network diagram showing DMZ vs. internal vs. OT segments, (3) list of internet-facing systems (from firewall ruleset export or WAF logs), (4) business continuity documentation identifying critical systems.

Step 3: If available, review the Zero Day Initiative's February 2026 Security Update Review for Patch Tuesday-specific context, particularly for Microsoft products and any vendor advisories released in the same window.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.2 (Patch Management as Preventive Measure)

Controls: NIST SI-2 - Flaw Remediation, CIS 7.3 - Address Unauthorized Software

Compensating: If ZDI report is paywalled: monitor Microsoft Security Update Guide (msrc.microsoft.com) directly on Patch Tuesday dates; enable RSS feed alerts. For non-Microsoft vendors, subscribe to their CVE notification channels via email or RSS. Document Patch Tuesday schedule (typically second Tuesday of each month) in your patching SLA, and use the 'lower volume window' to accelerate patch testing cycles—schedule test-to-production promotion immediately for any CVEs matching your Step 2 prioritization list.

Evidence: Before reviewing patch context: (1) export your current patch management system's 'pending patches' report filtered by CVSS ≥9.0 and status 'tested but not deployed', (2) list of Patch Tuesday deployment windows for the last 3 months (to identify any backlog), (3) business change calendar for February (to identify deployment blackout dates).

Step 4: Use the lower-volume month as an opportunity to close remediation gaps from January. A 43% drop in new critical disclosures is a relative reprieve, not a reduced threat posture; outstanding patches from prior months remain exploitable.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.3 (Post-Incident Activities, applied proactively to backlog)

Controls: NIST SI-2(3) - Flaw Remediation Verification, CIS 7.3 - Address Unauthorized Software

Compensating: Manually audit patch backlog: pull 'pending patches > 30 days old' from your patch management tool (or export deployed vs. available versions from vulnerability scanner), filter by CVSS ≥7.0, and group by system and business owner. Create a 'February Backlog Closure' task in your project management system, assign owners, and set deployment deadlines (e.g., all CVSS 9+ by Feb 14, all 7-9 by Feb 28). Track with weekly status emails to stakeholders.

Evidence: Capture before backlog closure: (1) current vulnerability scanner output showing all unpatched systems, (2) patch management tool report of 'patches released > 30 days ago, not yet deployed', (3) business impact assessment for each deferred patch (why was it deferred? test failure? compatibility? business exemption?), (4) list of systems with extended ESU (Extended Support Updates) or custom patch schedules.

Step 5: Brief security leadership and relevant stakeholders with a framing note: monthly CVE volume fluctuates based on disclosure cadence, not attacker activity. Avoid presenting the drop as a risk reduction without qualifying that interpretation.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §3.4 (Lessons Learned and Communications)

Controls: NIST IR-6 - Incident Reporting, CIS 6.1 - Establish and Maintain a Cybersecurity Awareness Program

Compensating: Create a one-page executive briefing template: (1) headline: 'February 2026 CVE Activity: 13 Critical Disclosures (43% Down from January)', (2) framing: 'Monthly volume reflects vendor disclosure timing and coordinated release schedules, not threat reduction', (3) actions: 'Completed X of Y prioritized patches; Y outstanding critical items due by [date]', (4) risk: 'Unpatched systems from prior months remain exploitable; patch backlog closure is priority', (5) metrics: 'Current unpatched rate: X%; target: <5% for CVSS ≥9.0 within 30 days'. Distribute via email with a 'reply with questions' invitation to create engagement.

Evidence: Prepare for the brief: (1) graph of CVE volume trend (Jan-Feb and YoY if available, sourced from NVD or your SIEM), (2) your current patch compliance dashboard (% systems patched by CVSS tier), (3) list of active exploits in the wild for any of the 13 CVEs (from threat feeds or CISA KEV), (4) business risk register showing which of your prioritized CVEs would have the highest business impact if exploited.

Step 6: Monitor for follow-on exploitation reporting, CISA KEV updates, vendor incident disclosures, and threat intelligence feeds to identify if any of the 13 critical CVEs move from disclosed to actively exploited status.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 (Detection and Analysis), applied to real-time CVE monitoring

Controls: NIST SI-4 - Information System Monitoring, NIST SI-4(16) - Threat Intelligence, CIS 8.1 - Establish a Security Awareness Program

Compensating: Set up free monitoring: (1) CISA KEV feed (cisa.gov/known-exploited-vulnerabilities) — subscribe to RSS/JSON API and check daily for any of the 13 CVEs; (2) Exploit-DB alerts (exploitdb.com) — search each CVE ID weekly for public PoC code; (3) Twitter/X saved search: 'exploit + [CVE-XXXX]' for each of the 13 CVEs, checked 2x weekly; (4) configure your SIEM to alert on any log patterns matching the CVE descriptions (e.g., specific payloads, affected endpoints, suspicious processes). Document findings in a shared tracking spreadsheet with columns: CVE ID, First PoC Date, First Exploit-in-the-Wild Report, Affected Systems in Your Environment, Patch Status, and Action Taken.

Evidence: Before starting monitoring: (1) establish baseline of current detection rules in your SIEM that cover vulnerability exploitation (search for rule tags like 'exploitation', 'cve-xxxx'), (2) export current threat intelligence feed list (IPs, domains, hashes known to be associated with active CVE exploitation), (3) document your alert thresholds (e.g., 'low noise tolerance for any PoC-to-active-exploit conversion'), (4) capture EDR/endpoint agent configuration for process/network alerting to detect exploitation attempts on unpatched systems.

Detection Guidance

Because the specific CVE IDs and affected products from the Insikt Group report are not reproducible from available source material, precise detection signatures cannot be provided here without risk of fabrication. The following guidance applies at the vulnerability management and monitoring layer:

Patch verification: Confirm that February 2026 vendor patches have been applied across affected systems. Query your vulnerability management platform for any assets still showing unpatched critical findings from the February disclosure window.

Exploitation attempt monitoring: For any critical CVEs confirmed in your environment after reviewing the full report, enable alerting on relevant exploitation patterns in your SIEM, particularly authentication failures, unusual

process spawning from service accounts, and lateral movement indicators following the affected system type (web application, OS kernel, network device, etc.).

Vendor advisory feeds: Subscribe to vendor security bulletins for any products confirmed in the 13 critical CVEs. Watch for vendor-issued indicators of exploitation or emergency re-patches.

CISA KEV tracking: Monitor the CISA Known Exploited Vulnerabilities catalog (cisa.gov/known-exploited-vulnerabilities-catalog) for any of the February 2026 critical CVEs being added; KEV addition is the highest-confidence signal that active exploitation is occurring in the wild.

Note: Specific IOC-level detection (hashes, IPs, domains) is not appropriate for this story given the absence of confirmed exploitation campaigns tied to the February 2026 critical CVEs in the available source material.

Framework Mappings

NIST-800-53R5

- **SI-2** — Flaw Remediation
- **IR-5** — Incident Monitoring

CIS-V8

- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

NIST-CSF-2

- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

Sources

Source	URL	Tier
Recordedfuture	https://www.recordedfuture.com/blog/february-2026-cve-landscape	T3
February 2026 CVE Landscape: 13 Critical Vulnerabilities Mark 43 ...	https://nemati.ai/blog/en-US/february-2026-cve-landscape-13-critica...	T3
February 2026 CVE Landscape: 13 Critical Vulnerabilities Mark 43 ...	https://www.instagram.com/p/DVys24zIK45/	T3
13 Critical Vulnerabilities Mark 43% Drop from January - X	https://x.com/Dinosn/status/2032298761586606215	T3

Source	URL	Tier
The February 2026 Security Update Review - Zero Day Initiative	https://www.thezdi.com/blog/2026/2/10/the-february-2026-security-up...	T3

Generated 2026-03-29 18:39 UTC by TJS Security Command Center