Executive Summary

Three new campaign to be reported this week. Key new entries this week: a DPRK-linked GitHub Actions supply chain campaign targeting healthcare CI/CD pipelines (CAMP.26.041), an active ransomware campaign by INC Ransom specifically targeting NHS and US hospital systems (CAMP.26.038), and an aloder Commvault backup server RCE zero-day (CVE-2025-34028) being actively exploited against healthcare organizations. **A key observation this week is that ransomware campaigns against healthcare are on the rise again with some very active attacks observed this past week.**

Medical Device & IoT Security section: CVE-2026-3650 (GDCM DICOM Memory Leak) Discussed in last week's brief still has no patch available. Continue applying compensating controls. The Contec CMS8000 backdoor (CVE-2024-12248 / CVE-2025-0626) and Texas HHSC directive were both covered in previous weeks brief. New this week: IoMT Exploitability Management framework (RSAC 2026).

Active Threat Campaigns- Healthcare & Technology

Campaign	Type	Key Techniques	Targets	Priority Action
DPRK GitHub Actions Supply Chain (CAMP.26.041)	Sabotage / Financial	Malicious GitHub Actions workflows inject credential-harvesting code into CI/CD pipelines; targets repos with healthcare EHR integrations and cloud-hosted data pipelines	Healthcare DevOps, Technology — US, EU	CRITICAL — Audit all GitHub Actions workflows for unauthorized changes; pin action versions to commit SHAs; rotate all CI/CD secrets immediately
INC Ransom Healthcare Targeting (CAMP.26.038)	Financial / Ransomware	Exploits Citrix Bleed (CVE-2023-4966) and unpatched FortiGate; deploys INC encryptor targeting EHR, PACS, and backup servers; double extortion	Healthcare, Critical Infrastructure — US, UK	HIGH — Patch Citrix/FortiGate immediately; verify INC-specific IOCs against EDR; test backup restoration; isolate PACS from general network.
Commvault Backup RCE Zero-Day (CVE-2025-34028)	Financial / Espionage	Unauthenticated RCE in Commvault Command Center (v11.36 and earlier); exploited by ransomware actors to destroy backups before encryption; CVSS 10.0	Healthcare, Enterprise IT — US, EU, AU	HIGH — Patch to v11.36.46+ immediately; isolate Commvault from internet; review backup job logs for unauthorized changes or deletions

Top 3 Actions This Week

1. [CRITICAL] Audit GitHub Actions Workflows — DPRK Supply Chain (CAMP.26.041)

A DPRK-nexus actor has been observed injecting malicious steps into GitHub Actions CI/CD workflows targeting healthcare organizations with cloud-connected EHR pipelines. The technique involves compromising a dependency workflow used across multiple repositories, allowing credential theft at build time without touching source code directly.

- Immediately audit all github/workflows/ files across your repositories for unauthorized additions or modifications — compare against last known-good commit
- Pin all GitHub Actions dependencies to specific commit SHAs (not floating tags like @v3) to prevent silent tag reassignment attacks
- Rotate all CI/CD secrets, including AWS access keys, GCP service accounts, container registry tokens, and any EHR API keys exposed in build environments
- Enable GitHub Actions audit logging and alert on any workflow file changes made by accounts outside your normal contributor group
- Review downstream artifact integrity — confirm that any container images or packages produced in the last 30 days were built from known-clean workflows

2. [HIGH] Patch Commvault Backup RCE (CVE-2025-34028) — CVSS 10.0

CVE-2025-34028 is an unauthenticated remote code execution vulnerability in Commvault Command Center (v11.36 and earlier), carrying a CVSS score of 10.0. Ransomware operators — including INC Ransom affiliates — are actively exploiting this to destroy or encrypt backup repositories before deploying ransomware on the primary environment, eliminating the victim's recovery options.

- Patch Commvault Command Center to v11.36.46 or later immediately — this is an unauthenticated RCE with no workaround
- Isolate all Commvault management interfaces from internet-facing networks pending patching
- Review backup job history for unexpected deletions, modifications, or access from unfamiliar IPs in the last 30 days
- Maintain at least one immutable, air-gapped backup copy that Commvault (or any backup management system) cannot reach

3. [HIGH] Defend Against INC Ransom Healthcare Targeting (CAMP.26.038)

INC Ransom has launched a targeted campaign against NHS trusts in the UK and US hospital systems, exploiting Citrix Bleed (CVE-2023-4966) and unpatched FortiGate appliances as initial access vectors. The group specifically targets EHR databases and PACS/radiology systems to maximize clinical disruption and ransom pressure.

- Verify Citrix NetScaler/ADC is patched against CVE-2023-4966 — this remains heavily exploited 18+ months after disclosure
- Patch all FortiGate appliances to current firmware — check CISA KEV for specific versions being exploited
- Segment EHR and radiology networks (PACS) from general corporate networks with explicit firewall allow-rules
- Verify EDR is deployed and active on all clinical endpoints including imaging workstations — INC uses custom encryptors that may bypass signature-based AV
- Test backup restoration for EHR and PACS systems — confirm you can fully recover within your RTO

Medical Device and IoT Security

GTI Intelligence Note: Medical Device Threat Landscape (April 2026)

GTI data confirms both CVE-2024-12248 (Contec CMS8000 RCE, CVSS 9.8) and CVE-2025-0626 (Contec backdoor) carry **No Known Exploitation** status as of April 10, 2026 per Google Threat Intelligence EPSS scoring. EPSS score for CVE-2024-12248 is 0.0068 (low active exploitation probability). However, GTI flags both as **HIGH risk** due to their healthcare OT targeting and absence of any available patch. The FDA recommendation to disconnect affected devices remains in force. Both of these were in the previous weeks threat intel brief if you need additional details.

IoMT Exploitability Management — New RSAC 2026 Framework (Medical Device)

New guidance presented at RSAC 2026 (Claroty/MultiCare) introduces an exploitability-first approach for managing the 89% of healthcare-connected medical devices carrying known CVEs that cannot be conventionally patched. This is a net-new framework not covered in prior briefs.

- Shift IoMT vulnerability prioritization away from CVSS scores alone — cross-reference your device CVE backlog against CISA's KEV catalog and EPSS exploitation probability scores
- For unpatchable legacy devices, focus on making devices unexploitable via network isolation, firewall rules, and traffic inspection rather than waiting for vendor patches
- Prepare for HIPAA Security Rule update expected to finalize May 2026 — network segmentation for medical devices will move from addressable to required

Ensure all IoMT devices are on dedicated, monitored VLANs with no direct internet connectivity — this is both the best compensating control and the upcoming compliance requirement

Sources: Google Threat Intelligence (GTI), CISA, FDA, MITRE ATT&CK, RSAC 2026, Health-ISAC, Cybersecurity Dive

Report suspicious activity to your IT security team immediately