INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-02 18:34 UTC

Weekly Vulnerability Roundup: 1,452 CVEs Tracked Including AI, VMware, ICS, and EV Flaws

SECURITY ANALYSIS | CRITICAL

SCC Item ID	SCC-STY-2026-0044
Type	Security Analysis
Severity	CRITICAL
Affected Products	Multiple platforms: VMware ESXi, ICS/SCADA systems, AI/ML frameworks, EV infrastructure, enterprise software
Published	12 hours ago
Discovery Source	Serper

Executive Summary

In a single reporting week, Cyble tracked 1,452 vulnerabilities across enterprise, operational technology, and emerging technology environments, with 222 publicly available proof-of-concept exploits dramatically shortening the window between disclosure and exploitation. A previously disclosed 2024 VMware flaw has moved into active exploitation, while newly cataloged weaknesses in ICS/SCADA systems, AI/ML platforms, and EV charging infrastructure signal that attackers are systematically probing every layer of the modern enterprise. The sheer volume of PoC-backed vulnerabilities, combined with CISA KEV additions, means security teams cannot prioritize reactively - they need continuous exposure management programs that map asset inventory to emerging threats in near real time.

Technical Analysis

The Cyble weekly digest covering the April 1 reporting period reflects a threat landscape defined by breadth rather than depth: 1,452 total CVEs, 150 of them specific to ICS environments, with 222 proof-of-concept exploits publicly accessible. That PoC ratio (roughly one in six disclosed vulnerabilities) is operationally significant - PoC availability compresses median time-to-exploitation, moving the burden from attacker capability to attacker targeting decisions.

The VMware ESXi flaw, originally disclosed in 2024, entering active exploitation follows a pattern well-documented in CISA KEV data: enterprise virtualization platforms are high-value targets because a single hypervisor compromise can yield lateral access across dozens of guest workloads. SecurityWeek's coverage corroborates active attacker interest, consistent with MITRE ATT&CK technique T1190 (Exploit Public-Facing Application) as the initial access vector and T1068 (Exploitation for Privilege Escalation) as the likely follow-on in

hypervisor contexts. VMware ESXi vulnerabilities have historically been weaponized by ransomware operators, most notably in the ESXiArgs campaign of 2023, making prompt patching and hypervisor isolation non-negotiable.

The 150 ICS-specific vulnerabilities represent a persistent structural problem in operational technology environments: OT asset owners frequently cannot patch on the same cadence as IT teams due to uptime requirements, vendor support constraints, and legacy system limitations. Manufacturing and critical infrastructure sectors carry disproportionate risk here. MITRE ATT&CK for ICS (T1203, Exploitation of Remote Services) applies directly: attackers exploiting unpatched ICS components can disrupt physical processes, not just data systems.

The AI/ML platform vulnerabilities and EV charging infrastructure flaws represent emerging attack surfaces that most enterprise security programs have not yet formally threat-modeled. AI/ML weaknesses can affect model integrity, training pipeline security, and inference API exposure - categories that sit at the intersection of software security and data integrity. EV charging flaws carry both operational and physical safety implications, as charging station networks often connect to backend management systems via internet-accessible APIs.

Source quality for this story is limited. The primary source is a Cyble blog digest; specific CVE identifiers, CVSS scores, and affected version strings were not available in the raw data. Claims in this analysis are scoped accordingly: the vulnerability counts, PoC figures, and sector coverage reflect Cyble's reported numbers, not independently verified CVE database queries. CISA's KEV catalog is the authoritative, independently verifiable reference for confirmed exploitation status.

Action Checklist

1. Step 1: Assess exposure. Audit your VMware ESXi inventory immediately; identify version strings and cross-reference against CISA's KEV catalog (cisa.gov/known-exploited-vulnerabilities-catalog) to confirm whether the specific 2024 flaw applies to your environment.
2. Step 2: Assess exposure (OT/ICS). If your organization operates or connects to ICS/SCADA environments, engage your OT security team or vendor to enumerate the 150 ICS CVEs flagged in this report against your installed base; Dragos or Claroty asset visibility tooling can accelerate this.
3. Step 3: Review controls. For VMware ESXi environments, verify network segmentation between hypervisor management interfaces and production workloads, confirm that ESXi management ports (443, 902) are not internet-exposed, and validate that vCenter access requires MFA.
4. Step 4: Review controls (PoC exposure). With 222 PoCs publicly available, prioritize patching by exploitability, not CVSS score alone; cross-reference open vulnerabilities against EPSS scores via FIRST.org to identify which unpatched CVEs carry the highest near-term exploitation probability.
5. Step 5: Update threat model. Formally add AI/ML platform attack surfaces and EV charging infrastructure to your asset register and threat model if your organization develops, operates, or procures from these categories; assign ownership for ongoing monitoring.
6. Step 6: Communicate findings. Brief leadership on the VMware active exploitation status with specific business context: what workloads run on affected hypervisors, what the blast radius of a compromise would be, and what the patching timeline looks like.
7. Step 7: Monitor developments. Track CISA KEV additions weekly; subscribe to Cyble, SecurityWeek, and CISA advisories for follow-on disclosures related to the specific CVEs in this reporting period as full technical details become available.

Detection Guidance

For VMware ESXi exploitation (T1190, T1068): review ESXi host logs for unexpected authentication attempts against the vSphere API or ESXi Shell; alert on SSH sessions to ESXi hosts outside of approved maintenance windows; monitor for new virtual machine creation, snapshot deletion, or datastore modification events not tied to change management tickets. SIEM queries should target ESXi syslog forwarding - if ESXi hosts are not forwarding logs to your SIEM, that gap requires immediate remediation before detection is meaningful.

For ICS environments: monitor historian and HMI access logs for connections originating outside defined engineering workstation IP ranges; alert on any remote access sessions to PLCs or RTUs not initiated through your approved jump server or OT DMZ; review firewall logs for direct IT-to-OT lateral traffic that bypasses the demilitarized zone.

For AI/ML platforms: audit API gateway logs for anomalous inference request volumes or unusual input patterns that may indicate prompt injection or model extraction attempts; review access logs for model training pipelines and data stores.

For PoC-backed vulnerabilities broadly: if your organization does not currently run a vulnerability management program that ingests EPSS scores alongside CVSS, this week's 222-PoC count is a concrete signal to build that capability. High EPSS + public PoC + CISA KEV listing is your triage priority stack.

Framework Mappings

MITRE-ATTACK

- **T1068** — Exploitation for Privilege Escalation
- **T1203** — Exploitation for Client Execution
- **T1190** — Exploit Public-Facing Application

NIST-800-53R5

- **AC-6** — Least Privilege
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-7** — Software, Firmware, and Information Integrity
- **IR-5** — Incident Monitoring

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.23** — Information security for use of cloud services

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1068	Exploitation for Privilege Escalation	Privilege-Escalation
T1203	Exploitation for Client Execution	Execution
T1190	Exploit Public-Facing Application	Initial-Access

Sources

Source	URL	Tier
	https://cyble.com/blog/cyble-weekly-vulnerabilities-report-apr-01/	T3
2024 VMware Flaw Now in Attackers' Crosshairs - SecurityWeek	https://www.securityweek.com/2024-vmware-flaw-now-in-attackers-cros...	T3
Known Exploited Vulnerabilities Catalog - CISA	https://www.cisa.gov/known-exploited-vulnerabilities-catalog	T1
VMware zero-day, manufacturing breaches, AI malware - Authentic8	https://www.authentic8.com/blog/cyber-intel-brief-vmware-zero-day-m...	T3
VMware ESXi Zero-Days Exploited for a Year — CISO Lessons	https://www.cloudsecuritynewsletter.com/p/vmware-esxi-zero-days-exp...	T3

Generated 2026-04-02 18:34 UTC by TJS Security Command Center