INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-19 13:51 UTC

CVE-2026-8153: Critical Vulnerability in Universal Robots PolyScope 5 Exposes Industrial Robot Fleets

CVE VULNERABILITY | CRITICAL

SCC Item ID	SCC-CVE-2026-0195
Type	CVE Vulnerability
CVE ID	CVE-2026-8153
Severity	CRITICAL
EPSS Score	0.0153 (82th percentile)
Affected Products	Universal Robots PolyScope 5 (specific versions unconfirmed, source is serper/news, not NVD)
Published	11 hours ago
Discovery Source	Serper

Executive Summary

A critical vulnerability in Universal Robots PolyScope 5, the control software for widely deployed collaborative robot arms, has been publicly reported. If confirmed, it would be remotely exploitable and pose risk to cobot fleets in manufacturing, logistics, and healthcare environments. Organizations should treat this as a priority inventory and exposure assessment pending vendor and NVD confirmation. Important: Technical claims in this report are unverified by NVD, CISA, or Universal Robots as of 2026-03-04.

Technical Analysis

CVE-2026-8153 has been publicly reported as affecting Universal Robots PolyScope 5, the programming and control platform for UR cobot arms. The report claims remote exploitability and potential to compromise robot operations. As of 2026-03-04, no official NVD record, CISA KEV entry, or Universal Robots security advisory has been published confirming the vulnerability, affected versions, vulnerability class (CWE), CVSS score, or exploitation details. The MITRE ATT&CK technique mapped is T1210 (Exploitation of Remote Services), consistent with network-accessible control software. EPSS score is 0.0153 at the 81.5th percentile, indicating elevated relative risk among unscored CVEs despite the absence of an official CVSS base score. Qualitative rating 'critical' is based on published severity claims and EPSS percentile; official CVSS validation from NVD is pending. All current sources are T3 (news, social media); no T1 authoritative confirmation exists. Operators

must monitor NVD (https://nvd.nist.gov/vuln/detail/CVE-2026-8153) and Universal Robots security advisory page (https://www.universal-robots.com/articles/ur/product-security/) for authoritative confirmation before executing version-specific remediation. Critical caveat: Technical claims in this entry should not be acted upon as confirmed risk until NVD or Universal Robots publishes an authoritative record.

Action Checklist

1. Step 1: Containment, Immediately inventory all systems running Universal Robots PolyScope 5 and identify their network exposure. Restrict PolyScope controllers from internet-facing access and isolate them within dedicated OT/ICS network zones. Enforce firewall rules limiting access to trusted sources only. This step is precautionary pending vendor confirmation; do not wait for official guidance to inventory and segment.
2. Step 2: Detection, Review network logs for unexpected inbound connections to PolyScope controller IPs on ports used by UR's communication interfaces (TCP 29999, 30001-30004, 502 Modbus). Flag any connections from external or untrusted IP ranges. PolyScope does not natively generate SIEM-compatible logs; rely on perimeter firewall and IDS telemetry. Check for anomalous robot behavior: unexpected motion programs, unauthorized parameter changes, or controller reboots. Document baseline behavior for post-patch comparison.
3. Step 3: Eradication, Monitor Universal Robots' official security advisory page for a confirmed patch or firmware update. Do not apply unofficial patches or third-party mitigations. While awaiting vendor guidance, maintain network segmentation controls from Step 1. Once an official patch is published, follow the vendor-specified upgrade path for PolyScope 5 and test in a non-production environment first.
4. Step 4: Recovery, After applying the vendor patch, verify controller integrity: confirm firmware version matches the patched release, review active motion programs for unauthorized modifications, and validate that network access controls remain in place. Monitor cobot behavior for a minimum of 72 hours post-remediation for anomalies.
5. Step 5: Post-Incident, Assess whether PolyScope controllers are unnecessarily network-exposed. Apply IEC 62443 zone-and-conduit network segmentation if not already in place. Document this event as a case study for OT/ICS asset inventory maturity and consider adding UR controllers to continuous OT monitoring tooling.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to OT security leadership and consider regulatory notification if forensic evidence (unauthorized `.urp` programs, unexpected controller reboots, anomalous motion events, or unauthorized SSH keys) confirms active exploitation of any PolyScope 5 controller, or if any controller was confirmed reachable from an internet-facing network segment prior to isolation — particularly in healthcare environments where cobot compromise may trigger FDA medical device incident reporting obligations or manufacturing environments with safety system integration.

Recovery Notes	After patching, do not restore PolyScope controllers to pre-incident network configurations — validate and enforce OT VLAN segmentation as the new baseline before returning cobots to production. Monitor perimeter firewall logs for outbound connections from controller IPs for a minimum of 72 hours, as a persistent implant (e.g., a reverse shell planted via URScript or a modified PolyScope service binary) would survive a firmware patch if it achieved persistence in the `/programs/` directory or via a cron job. Treat any motion anomaly — unexpected joint movement, unauthorized speed-override changes, or safety-limit modifications observed on the teach pendant — during the monitoring window as an indicator of active compromise requiring immediate re-isolation.
Forensic Artifacts	Perimeter firewall flow logs (NetFlow/syslog) for PolyScope controller IPs on TCP 29999 (Dashboard Server), 30001 (Primary Client), 30002 (Secondary Client), 30003 (Real-Time Client), 30004 (RTDE), and TCP 502 (Modbus) — these are the only interfaces through which CVE-2026-8153 remote exploitation could have occurred, and connection records to non-OT sources are the primary indicator of pre-patch access. | PolyScope controller filesystem artifacts: `/programs/*.urp` and `/programs/*.script` files with modification timestamps outside scheduled maintenance windows — an attacker leveraging remote code execution on PolyScope would most likely establish persistence by planting a malicious URScript motion program or modifying an existing one to execute shell commands via the `system()` URScript function. | SSH authentication logs at `/var/log/auth.log` on each PolyScope controller — successful SSH logins from unexpected source IPs or at anomalous times, and the contents of `/root/.ssh/authorized_keys`, would indicate the attacker established persistent remote access following initial exploitation. | Pre-patch forensic image (dd) of the PolyScope controller storage media — required to preserve evidence of any modified system binaries, added cron jobs (`/var/spool/cron/` or `/etc/cron.d/`), or planted reverse-shell scripts that the official firmware patch would overwrite, particularly relevant if the vulnerability enables arbitrary file write or RCE on the underlying Linux OS. | Modbus TCP packet captures from a SPAN port on the OT switch — raw Modbus frames will record any unauthorized coil writes (robot enable/disable), holding register modifications (speed overrides, safety boundaries), or diagnostic function code (FC 8) abuse that an attacker used to manipulate robot behavior, separate from the initial exploitation vector.

Per-Action IR Details

Step 1: Containment — Immediately inventory all systems running Universal Robots PolyScope 5. Isolate cobot controllers from internet-facing network segments and restrict access to trusted OT/ICS network zones. Do not wait for NVD confirmation given the critical severity rating and remote exploitation claim.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Run a network sweep with `nmap -p 29999,30001-30004,502 --open -oN ur_polyscope_hosts.txt` to enumerate all reachable PolyScope controllers without relying on asset management tooling. Cross-reference output against any existing OT network diagrams. Immediately apply ACLs at the nearest managed switch to drop inbound traffic to those ports from non-OT VLANs — no SIEM required.

Evidence: Before isolating, capture the current ARP table (`arp -a` on the network gateway) and a full packet capture on the OT segment interface using `tcpdump -i -w ur_pre_isolation_$(date +%Y%m%d%H%M).pcap host ` for at least 5 minutes. This baseline preserves any active C2 sessions or lateral movement traffic targeting PolyScope's TCP 29999 (dashboard server) or 30001–30004 (real-time/secondary/primary client) interfaces that would be severed by isolation.

Step 2: Detection — Review network logs for unexpected inbound connections to PolyScope controller IPs on ports used by UR's communication interfaces (TCP 29999, 30001-30004, 502 Modbus). Flag any connections from external or untrusted IP ranges. PolyScope does not natively generate SIEM-compatible logs; rely on perimeter firewall and IDS telemetry. Check for anomalous robot behavior: unexpected motion programs, unauthorized parameter changes, or controller reboots.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: On the perimeter firewall or OT-facing router, export connection logs filtered for destination IPs of all PolyScope controllers on ports 29999, 30001–30004, and 502, then pipe through `grep` or `awk` to isolate source IPs outside the approved OT subnet range. Deploy Wireshark on a network tap or SPAN port pointed at the OT segment and capture a 1-hour baseline: filter on `tcp.port in {29999 30001 30002 30003 30004} or modbus`, looking for URScript command payloads (plain-text ASCII over TCP 30001) that include motion commands (`movej`, `movel`, `set_digital_out`) issued outside normal production windows. On the PolyScope teach pendant, manually inspect `/programs/` directory via SSH (if enabled) or the file manager for `.urp` program files with modification timestamps outside scheduled maintenance windows.

Evidence: Collect perimeter firewall flow logs (NetFlow or syslog) filtered on PolyScope controller IPs for the 30 days prior to advisory publication. Pull the PolyScope controller's `/var/log/` directory contents via SSH — specifically `syslog`, `auth.log`, and any UR daemon logs — before any changes are made. Capture `/programs/*.urp` and `/programs/*.script` file metadata (modification timestamps, file hashes via `md5sum`) to detect injected or altered motion programs. If Modbus (TCP 502) traffic is present, capture raw frames to identify unauthorized register reads/writes targeting coil addresses that map to robot enable or speed-override functions.

Step 3: Eradication — Monitor Universal Robots' official security advisory page (https://www.universal-robots.com/articles/ur/product-security/) for a confirmed patch or firmware update. Do not apply unofficial mitigations. Once an official patch is published, follow the vendor-specified upgrade path for PolyScope 5. Specific version ranges are unconfirmed at this time.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST CM-3 (Configuration Change Control), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: Until UR publishes an official patch, implement the following manual compensating controls: (1) Disable the PolyScope remote access interface by navigating to Settings > System > Network on the teach pendant and disabling the 'Remote Control' toggle if not operationally required. (2) Block TCP 29999, 30001–30004, and 502 at the OT VLAN ACL for all sources except explicitly whitelisted engineering workstation IPs. (3) Subscribe to UR's security advisory RSS feed or configure a free change-detection alert via a service such as visualping.io pointed at the UR product security page, so patch publication triggers an immediate notification without requiring manual polling.

Evidence: Before applying any patch, image the PolyScope controller's eMMC or SD storage using `dd if=/dev/mmcblk0 of=/mnt/usb/polyscope_pre_patch_$(hostname)_$(date +%Y%m%d).img bs=4M` (adjust device path per UR hardware model) to preserve a forensic baseline. Hash the image with `sha256sum` and store it offline. This preserves any attacker-planted URScript backdoors, modified system binaries, or unauthorized SSH authorized_keys entries in `/root/.ssh/authorized_keys` that patching would overwrite.

Step 4: Recovery — After applying the vendor patch, verify controller integrity: confirm firmware version matches the patched release, review active motion programs for unauthorized modifications, and validate that network access controls remain in place. Monitor cobot behavior for a minimum of 72 hours post-remediation.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST SI-7 (Software, Firmware, and Information Integrity), NIST CA-7 (Continuous Monitoring), NIST IR-4 (Incident Handling), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: Post-patch, verify the installed PolyScope version via the teach pendant under About > Software Version and cross-check against the version string in UR's advisory. Enumerate all `.urp` motion program files under `/programs/` and generate SHA-256 hashes (`find /programs -name '*.urp' -exec sha256sum {} \; > /tmp/programs_post_patch_hashes.txt`), then diff against pre-patch hashes to identify any files modified during the incident window. For 72-hour behavioral monitoring, configure your OT firewall to alert on any new outbound connection attempts originating from PolyScope controller IPs — a compromised controller establishing reverse-shell or C2 beaconing over TCP would be anomalous post-isolation and is the primary indicator of persistent implant activity.

Evidence: Collect a post-patch network flow snapshot to confirm no outbound connections from PolyScope controller IPs to non-OT destinations. Verify `/root/.ssh/authorized_keys` and `/etc/passwd` on each controller for unauthorized accounts or SSH keys added during the exploitation window. Check PolyScope's installation log at `/var/log/dpkg.log` or equivalent for any package modifications outside the official patch installation event.

Step 5: Post-Incident — Assess whether PolyScope controllers are unnecessarily network-exposed. Apply IEC 62443 zone-and-conduit network segmentation if not already in place. Document this event as a case for OT/ICS asset inventory maturity and consider adding UR controllers to continuous OT monitoring tooling.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SC-7 (Boundary Protection), NIST RA-3 (Risk Assessment), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: Deploy Dragos Community Edition or Claroty free-tier (where available) for passive OT asset discovery and protocol anomaly detection on the UR cobot VLAN going forward — both support Modbus and proprietary UR TCP protocol fingerprinting without requiring active scanning that could disrupt robot operations. Alternatively, configure a dedicated Zeek (formerly Bro) sensor on a SPAN port of the OT switch with the Modbus and DNP3 protocol analyzers enabled; Zeek's `modbus.log` will capture all register reads/writes to PolyScope controllers, providing an audit trail that PolyScope itself does not natively generate. Document the IEC 62443 zone-and-conduit model for the robot cell, designating PolyScope controllers as Security Level 2 targets requiring conduit firewalling from the enterprise IT network.

Evidence: Produce a lessons-learned report documenting: (1) the time delta between CVE public reporting and PolyScope controller inventory completion — this gap represents your detection blind spot for OT assets; (2) whether any PolyScope controller was reachable from outside the OT VLAN prior to this event, evidenced by pre-incident firewall flow logs; (3) the total count of PolyScope 5 controllers discovered during Step 1 inventory versus what was recorded in the CMDB, to quantify OT asset inventory gaps for future remediation prioritization.

Detection Guidance

Detection guidance below is based on attack surface analysis of UR PolyScope control interfaces and T1210 exploitation patterns. These recommendations are speculative pending confirmed technical details from Universal Robots; adjust rule tuning once an advisory is published. No confirmed IOCs (indicators of compromise) are available. Detection relies on network-layer telemetry. Monitor firewall and IDS logs for inbound connections to Universal Robots controller IPs on UR communication ports (TCP 29999, 30001, 30002, 30003, 30004) and Modbus TCP port 502 from untrusted or external sources. Alert on any new or unexpected source IPs accessing these ports. On the OT side, watch for anomalous robot behavior: unscheduled program execution, unexpected joint movements, unauthorized safety parameter changes, or controller reboots without operator action. If a SIEM is ingesting OT network flow data, create a detection rule for external-to-OT lateral movement consistent with T1210 (Exploitation of Remote Services). Absence of confirmed IOCs reflects the current lack of published technical detail from vendors, not absence of risk.

Framework Mappings

MITRE-ATTACK

- **T1210** — Exploitation of Remote Services

NIST-800-53R5

- **AC-6** — Least Privilege
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation

ISO-27001-2022

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1210	Exploitation of Remote Services	Lateral-Movement

Sources

Source	URL	Tier
	https://www.securityweek.com/critical-vulnerability-exposes-industr...	T3
Critical Vulnerability Exposes Industrial Robot Fleets to Hacking	https://x.com/TheCyberSecHub/status/2056621690621436302	T3
Critical Vulnerability Exposes Universal Robots' Cobots to Remote ...	https://www.reddit.com/r/pwnhub/comments/1thlvlw/critical_vulnerabi...	T3
Critical Vulnerability Exposes Industrial Robot Fleets to Hacking	https://www.show.it/critical-vulnerability-exposes-industrial-robot...	T3
Critical Vulnerability Exposes Industrial Robot Fleets to Hacking	https://x.com/SecurityWeek/status/2056621222750732423	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-8153	T1

Generated 2026-05-19 13:51 UTC by TJS Security Command Center