



# OT-ISAC

OPERATIONAL TECHNOLOGY INFORMATION SHARING AND ANALYSIS CENTER

## OT-ISAC VULNERABILITY ADVISORY

TLP:CLEAR – Information may be distributed freely, subject only to copyright controls.

*In the spirit of community-driven effort, we'd like to encourage our Members and Partners to share information to enable our community better to defend itself and improve situational awareness. **Most importantly - If your organization require direct assistance from OT-ISAC, feel free to submit to OT-ISAC Member's Portal- our team will work with you to ensure all necessary support is available through the member submission and RFI process.***

**Disclaimer: This information is provided as-is for informational purposes only and comes with no expressed or implied warranties. While efforts have been made to ensure the accuracy and reliability of the information, the evolving nature of cybersecurity threats means that vulnerabilities, impacts, and best practices may change over time. You (and any individual or entity you represent) bear full responsibility for all actions and omissions made based on this information. OT-ISAC disclaims any responsibility or liability for any such actions or omissions.**

<b>Source Advisories:</b>	ICSA-26-099-01 to -02; Mitsubishi Electric GENESIS64 and ICONICS Suite products; Siemens April advisory batch; ICSA-26-106-01 to -04.
<b>Initial Release:</b>	17 April 2026
<b>Advisory Date:</b>	17 April 2026
<b>Classification:</b>	TLP:CLEAR – Information may be distributed freely, subject only to copyright controls.
<b>Severity:</b>	CRITICAL / HIGH – See Vulnerability Summary

## Executive Summary

This TLP:CLEAR compilation brings together the core April 2026 vulnerability items previously covered across OT-ISAC advisories and one Mitsubishi Electric product note. The included disclosures affect legacy BACnet field controllers, gas odorization platforms, HMI and historian software, industrial wireless infrastructure, OT network-management and remote-access systems, engineering workstations, PLC ecosystems, OT-adjacent access-control products, and pipeline training simulation infrastructure.

The most operationally significant issues in this set are the obsolete BASControl20 flaw with no published fix, the AVEVA Pipeline Simulation authorization bypass, the Horner weak-password issue affecting PLC and engineering workflows, the critical Anviz archive-based device compromise path, and the Siemens management-plane weaknesses affecting industrial communications and access-management layers. Mitsubishi GENESIS64 and ICONICS Suite remain important because local credential disclosure can still undermine historian integrity and OT-adjacent SQL-connected environments.

No public exploitation was reported to CISA at publication time across the source advisories. Several issues are still network-reachable and operationally relevant where exposure exists, so prioritization should be driven by asset criticality, reachability, and the presence of legacy or difficult-to-replace systems.

## At-a-Glance

Field	Detail
Risk Level	HIGH - multiple Critical issues across process, management-plane, engineering, and OT-adjacent access-control environments.
Confidence	BASControl20 (legacy/EOL), AVEVA Pipeline Simulation, Horner XL4/XL7 and Cscape, selected Siemens management-plane issues, and Anviz CX2 Lite/CX7/CrossChex.
Key Finding	Unauthenticated or weakly authenticated network access, management-plane abuse, protocol misuse, local credential disclosure, and malicious file or package handling.
Primary Action	Patch where fixes exist, isolate or replace obsolete systems, restrict network exposure, validate remote-access paths, and strengthen monitoring around management interfaces and unusual configuration changes.
Exploit status	No public exploitation reported to CISA at publication time across the source advisories referenced in this compilation.

## Vulnerability Summary

Product / family	Key CVE(s)	Severity	Exposure	OT/ICS significance	Priority action
Contemporary Controls BASControl20 / BASC 20T	CVE-2025-13926	<b>9.8 Critical</b>	Network sniff + forged packet requests; obsolete product	Legacy BACnet/IP field controller exposure with no published fix path	Isolate, apply compensating controls, and plan replacement
GPL Odorizers GPL750	CVE-2026-4436	<b>8.6 High</b>	Remote Modbus packet manipulation	Direct process and safety consequence through odorant injection logic	Apply latest GPL750 software and applicable Horner firmware; segment Modbus paths
Mitsubishi Electric GENESIS64 / ICONICS Suite / related products	CVE-2025-14815, CVE-2025-14816	<b>8.8 High</b>	Local credential disclosure through cache / GUI storage	Can expose SQL credentials and undermine historian, HMI, and analytics data integrity	Upgrade to fixed versions, disable local cache, delete cache files, rotate SQL credentials
Siemens SCALANCE W-700	CVE-2022-36323, CVE-2023-44373 plus related flaws	<b>9.1 Critical</b>	Management-plane command injection on industrial wireless devices	Compromise can affect industrial wireless communications carrying PLC, HMI, or plant traffic	Update to V6.6.0 and restrict management access
Siemens SINEC NMS	CVE-2026-25654, CVE-2026-24032	<b>8.8 / 7.3 High</b>	Authorization bypass and authentication bypass in centralized OT network management	High-value risk to credentials, password resets, and network operations governance	Update to V4.0 SP3 and review UMC deployments
Siemens Industrial Edge Management	CVE-2026-33892	<b>7.1 High</b>	Authentication bypass on remote connections	Can expose connected Industrial Edge devices through	Patch promptly and restrict or disable remote connection features

Product / family	Key CVE(s)	Severity	Exposure	OT/ICS significance	Priority action
			when feature is enabled	remote management pathways	
Siemens RUGGEDCOM CROSSBOW SAC / SAM-P	CVE-2025-6965, CVE-2026-27668	7.7 / 8.8 High	Memory corruption and privilege escalation in secure remote access stack	Important for utility and substation remote administration trust boundaries	Update to V5.8 and review administrator privileges
Delta Electronics ASDA-Soft	CVE-2026-5726	7.8 High	Local malicious .par file parsing	Engineering-workstation compromise risk for motion-control environments	Upgrade to v7.2.6.0+ and restrict untrusted project / parameter files
Horner Automation Cscape / XL4 / XL7	CVE-2026-6284	9.1 Critical	Weak password controls on reachable PLC / OCS ecosystem	Unauthorized access risk to PLC logic and associated services	Upgrade Cscape to v10.2 SP2+ and review XL4/XL7 exposure immediately
Anviz CX2 Lite / CX7 / CrossChex Standard	CVE-2026-35546 and related CVEs	9.8 Critical + multiple High	Unauthenticated archive-based device compromise, session exposure, and management-traffic weaknesses	OT-adjacent physical access systems can still affect trust, facility access, and management data integrity	Restrict or isolate exposed devices and management software; engage vendor and harden admin paths
AVEVA Pipeline Simulation	CVE-2026-5387	9.1 / 9.3 Critical	Unauthenticated API calls to privileged simulator functions	Can alter simulation parameters, training records, and operator-readiness workflows	Upgrade to 2025 SP1 P01+, restrict API access, and enable TLS

## Why It Matters to OT/ICS

- **Control-plane and management risk:** Several items affect the systems that manage or mediate industrial connectivity rather than field controllers directly. Siemens SINEC NMS, Industrial Edge Management, RUGGEDCOM CROSSBOW, SCALANCE W-700, and Horner control workflows all sit close to operational communications or remote-administration pathways.
- **Process and safety implications:** GPL750 can directly alter odorant injection logic, while BASControl20 remains a serious legacy controller issue where it is still deployed. AVEVA Pipeline Simulation does not directly control a live process, but compromise can still degrade training fidelity, exercise integrity, and operator-readiness assurance.
- **Engineering and data-trust impact:** Delta ASDA-Soft and Mitsubishi GENESIS64 / ICONICS Suite show that local or engineering-layer weaknesses still matter in OT because project workflows, historian data, cached credentials, and management visibility can all influence safe and reliable operations.
- **OT-adjacent security dependencies:** Anviz and CrossChex are not classic ICS controllers, but they are still relevant in industrial campuses because physical access systems, attendance systems, and supporting management servers can affect trust relationships, site access, and response workflows.

## Risk Assessment

This consolidated risk view reflects the current public reporting across the included April 2026 advisories and emphasizes exposure conditions, operational consequence, and the nature of the affected assets rather than novelty alone.

Dimension	Assessment
Threat Sophistication	Low to Moderate. Several attack paths are straightforward where the vulnerable service or device is reachable, though some issues still depend on local access, adjacent-network position, or authenticated workflow abuse.
Potential Impact	High. Included vulnerabilities span direct process and safety implications, PLC and management-plane access, engineering-workstation compromise, historian and data-integrity loss, and degradation of operator-training assurance.
Likelihood of Exploitation	Low in the immediate term based on public reporting at publication time, but Moderate over a 30–90 day window for reachable AVEVA, Horner, Anviz, and legacy BASControl20 deployments as understanding and testing of the flaws spreads.
Overall Risk	High. The compilation includes multiple Critical issues across process, management-plane, engineering, and OT-adjacent security systems, including one obsolete controller with no published fix path and several network-relevant attack surfaces.

## Operational Prioritization (SSVC-informed)

This public-facing prioritization condenses the underlying SSVC-style triage into a concise action view for unrestricted sharing. It is intended to help readers quickly identify which issues merit immediate action, accelerated remediation, or monitoring based on exposure, impact, and operational relevance.

Product / family	Priority	Why it matters most	Suggested public-safe action
AVEVA Pipeline Simulation	<b>Act</b>	Unauthenticated API operations can change simulation parameters, training configurations, and records. The issue is network-reachable and operationally meaningful in process-training environments.	Upgrade to 2025 SP1 P01 or later; restrict API access to trusted clients; enable TLS.
Horner Automation Cscape / XL4 / XL7	<b>Act</b>	Critical weak-password exposure affects PLC/HMI-class systems and associated engineering access where network reachability exists.	Upgrade Cscape to the fixed release; review password policy and reachable management paths immediately.
Contemporary Controls BASControl20 / BASC 20T	<b>Act</b>	The controller is obsolete, carries critical severity, and has no published vendor fix path. Residual risk remains high wherever legacy deployments persist.	Isolate from less-trusted networks, apply compensating controls, and plan replacement.
Anviz CX2 Lite / CX7 / CrossChex Standard	<b>Attend</b>	The most serious Anviz path is remote compromise of access-control devices; related CrossChex weaknesses can undermine management traffic and backend trust. Exposure is highly deployment-dependent.	Restrict or isolate exposed devices and management servers; reduce HTTP/admin exposure; engage the vendor directly.
GPL Odorizers GPL750; Mitsubishi GENESIS64 / ICONICS; Siemens April management-plane items; Delta ASDA-Soft	<b>Attend</b>	These issues matter for process safety, historian and engineering trust, and industrial network administration, but they are either more context-dependent, partially local, or better suited to accelerated maintenance planning than emergency response.	Apply vendor updates or mitigations, validate affected assets, and prioritize by network reachability and operational role.
Lower-severity reconnaissance and	<b>Track*</b>	Several issues support reconnaissance, credential exposure, or exploit chaining rather than standalone	Monitor for unusual camera/debug requests, archive uploads, cleartext

Product / family	Priority	Why it matters most	Suggested public-safe action
chaining items in the Anviz set		destructive impact. They still warrant tracking where the products are present.	admin sessions, and database anomalies.

## Priority Actions / Recommendations

Priority	Action
Immediate	Patch AVEVA Pipeline Simulation and Horner Cscape where present, isolate or replace BASControl20, review exposed Anviz/CrossChex assets, and update Siemens management-plane products with critical or high-risk fixes.
Accelerated	Apply Mitsubishi fixed versions and local-cache mitigations, update GPL750 software and firmware guidance, and review SCALANCE wireless management exposure.
Validation	Inventory affected assets, identify remote-access paths, test updates in maintenance windows, and confirm whether legacy or no-fix systems require compensating controls or replacement planning.
Monitoring	Increase scrutiny on unusual password-reset events, brute-force attempts, archive or update uploads, unexpected BACnet or Modbus writes, unauthenticated API activity, and changes to training or management-system configurations.

## Selected Detection Considerations

- Monitor for abnormal BACnet/IP controller-management traffic, forged requests, unexpected file-transfer-style actions, and unusual Modbus writes to odorant-injection logic.
- Alert on repeated Horner login failures or brute-force patterns, unusual password-reset activity in SINEC NMS, and anomalous administration of Siemens RUGGEDCOM or Industrial Edge management components.
- Watch for suspicious archive uploads, update-package activity, debug-information requests, unexpected HTTP administrative sessions, and CrossChex traffic manipulation on Anviz environments.
- Review engineering hosts for suspicious .par file handling, unusual child-process activity from ASDA-Soft, and unexpected access to Mitsubishi local cache files or SQL-connected services.
- Alert on unusual AVEVA Pipeline Simulation API calls, unexpected changes to simulation parameters or training records, and activity from non-standard clients or out-of-hours maintenance windows.

## Scope and Limitations

This report is a public-safe consolidation of previously covered items and therefore emphasizes current defensive relevance, affected assets, and remediation priorities rather than reproducing all member-only analytical sections from the original advisories.

No public exploitation was reported to CISA at publication time across the source advisories referenced here. Exploitation likelihood remains exposure-driven and can change quickly as proof-of-concept details or opportunistic scanning emerge.

Anviz remediation clarity remains limited in the source material because the vendor reportedly did not respond to CISA coordination attempts. BASControl20 is notable because the product is obsolete and no clear public patch path was stated in the advisory.

## Disclaimer

TLP:CLEAR HANDLING: This advisory is released under TLP:CLEAR and may be shared without restriction, subject to standard copyright rules. Recipients may distribute it publicly, including via websites, reports, presentations, and media engagement. The analytical sections – including Key Findings, OT-ISAC Analytical Assessment, SSSVC-informed Operational Prioritization, Risk Assessment, and Detection Considerations –

represent OT-ISAC’s analytical judgment and are provided to support broad defensive awareness across the community.

This advisory is provided for informational purposes only, based on publicly available source advisories published by CISA and original vendor security disclosures, combined with OT-ISAC analytical assessment. It is provided without expressed or implied warranties of any kind, including without limitation any warranties of accuracy, completeness, or fitness for purpose. The information reflects the state of open-source knowledge and OT-ISAC analysis as of 17 April 2026. OT-ISAC does not independently verify vendor claims, CVSS scores, or remediation guidance. Organisations remain solely responsible for all decisions taken in response to this advisory, including assessment of risk to their specific environments, compatibility of patches, and operational impact of any mitigations applied. This advisory should not be construed as legal, regulatory, or compliance guidance.

## References

---

1. CISA ICS Advisory ICSA-26-099-01 - Contemporary Controls BASC 20T
2. CISA ICS Advisory ICSA-26-099-02 - GPL Odorizers GPL750
3. Mitsubishi Electric / Mitsubishi Electric Iconics Digital Solutions - vulnerabilities in GENESIS64 and ICONICS Suite products
4. Siemens ProductCERT April 2026 advisories covering SCALANCE W-700, SINEC NMS, Industrial Edge Management, TPM 2.0, and RUGGEDCOM CROSSBOW
5. CISA ICS Advisories ICSA-26-106-01 to -04 covering Delta Electronics ASDA-Soft, Horner Automation Cscape and XL4/XL7 PLC, Anviz multiple products, and AVEVA Pipeline Simulation
6. Relevant vendor remediation guidance cited in the source advisories, including AVEVA Pipeline Simulation 2025 SP1 P01, Horner Cscape v10.2 SP2+, Delta ASDA-Soft v7.2.6.0+, Siemens fixed releases, and Mitsubishi local-cache cleanup steps

---

## End of Advisory

**Public note.** This TLP:CLEAR version is intended for unrestricted sharing. It retains only public-safe facts and concise OT/ICS prioritization, and does not reproduce member-only handling language or full internal analytical sections.