



## America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

### ICS ADVISORY

# Horner Automation Cscape and XL4, XL7 PLC

**Release Date:** April 16, 2026

**Alert Code:** ICSA-26-106-02

**RELATED TOPICS:** [INDUSTRIAL CONTROL SYSTEM VULNERABILITIES](#) </topics/industrial-control-systems/industrial-control-system-vulnerabilities>, [INDUSTRIAL CONTROL SYSTEMS](#) </topics/industrial-control-systems>

**View CSAF** <[https://github.com/cisagov/csaf/blob/develop/csaf\\_files/ot/white/2026/icsa-26-106-02.json](https://github.com/cisagov/csaf/blob/develop/csaf_files/ot/white/2026/icsa-26-106-02.json)>

## Summary

**Successful exploitation of this vulnerability could allow an attacker to gain unauthorized access to systems and services.**

The following versions of Horner Automation Cscape and XL4, XL7 PLC are affected:

- Cscape v10.0
- XL7 PLC v15.60
- XL4 PLC v16.32.0

CVSS	Vendor	Equipment	Vulnerabilities
v3 9.1	Horner Automation	Horner Automation Cscape and XL4, XL7 PLC	Weak Password Requirements

## Background

- **Critical Infrastructure Sectors:** Critical Manufacturing
- **Countries/Areas Deployed:** Worldwide
- **Company Headquarters Location:** United States

## Vulnerabilities

[Expand All +](#)

CVE-2026-6284



## Acknowledgments

- An anonymous researcher reported this vulnerability to CISA

## Legal Notice and Terms of Use

This product is provided subject to this Notification (<https://www.cisa.gov/notification>) and this Privacy & Use policy (<https://www.cisa.gov/privacy-policy>).

# Recommended Practices

CISA recommends users take defensive measures to minimize the risk of exploitation of this vulnerability.

Minimize network exposure for all control system devices and/or systems, ensuring they are not accessible from the internet.

Locate control system networks and remote devices behind firewalls and isolating them from business networks.

When remote access is required, use more secure methods, such as Virtual Private Networks (VPNs), recognizing VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is only as secure as the connected devices.

CISA reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

CISA also provides a section for control systems security recommended practices on the ICS webpage on [cisa.gov/ics](https://cisa.gov/ics). Several CISA products detailing cyber defense best practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.

CISA encourages organizations to implement recommended cybersecurity strategies for proactive defense of ICS assets.

Additional mitigation guidance and recommended practices are publicly available on the ICS webpage at [cisa.gov/ics](https://cisa.gov/ics) in the technical information paper, ICS-TIP-12-146-01B-- Targeted Cyber Intrusion Detection and Mitigation Strategies.

Organizations observing suspected malicious activity should follow established internal procedures and report findings to CISA for tracking and correlation against other incidents.

No known public exploitation specifically targeting this vulnerability has been reported to CISA at this time.

---

## Revision History

- **Initial Release Date:** 2026-04-16

Date	Revision	Summary
2026-04-16	1	Initial Publication

---

## Legal Notice and Terms of Use

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

## Vendor

- Horner Automation

### Tags

**Sector:** [Critical Manufacturing Sector](#)

**Topics:** [Industrial Control System Vulnerabilities](#), [Industrial Control Systems](#)

</topics/industrial-control-systems>



## Please share your thoughts

We recently updated our anonymous [product survey](#); we welcome your feedback.

## Related Advisories

APR 16, 2026 ■ ICS ADVISORY | ICSA-26-106-04

### [AVEVA Pipeline Simulation](#) </news-

[events/ics-advisories/icsa-26-106-04>](#)

APR 16, 2026 ■ ICS ADVISORY | ICSA-26-106-03

### [Anviz Multiple Products](#) </news-

[events/ics-advisories/icsa-26-106-03>](#)

APR 16, 2026 ■ ICS ADVISORY | ICSA-26-106-01

### [Delta Electronics ASDA-Soft](#)

[</news-events/ics-advisories/icsa-26-106-01>](#)

APR 09, 2026 ■ ICS ADVISORY | ICSA-26-099-02

### [GPL Odorizers GPL750](#) </news-

[events/ics-advisories/icsa-26-099-02>](#)

[Return to top](#)

[Topics](#)

[Spotlight](#)

[Resources & Tools](#)

[News & Events](#)

[Careers](#)

[About](#)



**CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY**



**CISA Central**

1-844-Say-CISA

[contact@cisa.dhs.gov](mailto:contact@cisa.dhs.gov)



CISA.gov

An official website of the U.S. Department of Homeland Security

[About CISA](#)

[Budget and Performance](#)

[DHS.gov](https://www.dhs.gov)

<https://www.dhs.gov/performance-financial-reports>

[FOIA Requests](#)

[No FEAR Act](#)

[Office of Inspector General](#)

<https://www.dhs.gov/foia>

<https://www.oig.dhs.gov>

[Privacy Policy](#)

[Subscribe](#)

[The White House](#)

<https://www.whitehouse.gov>

[USA.gov](https://www.usa.gov)

[Website Feedback](#)