America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

ICS ADVISORY

Horner Automation Cscape

Release Date: May 08, 2025 **Alert Code:** ICSA-25-128-01

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>

1. EXECUTIVE SUMMARY

- **CVSS v4 8.4**
- **ATTENTION**: Low attack complexity
- **Vendor**: Horner Automation
- **Equipment**: Cscape
- **Vulnerability**: Out-of-bounds Read

2. RISK EVALUATION

Successful exploitation of this vulnerability could allow an attacker to disclose information and execute arbitrary code.

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

The following versions of Horner Automation Cscape, a control system application programming software, are affected:

- Cscape: Version 10.0 (10.0.415.2) SP1

3.2 VULNERABILITY OVERVIEW

3.2.1 OUT-OF-BOUNDS READ CWE-125

<https://cwe.mitre.org/data/definitions/125.html>

Horner Automation Cscape version 10.0 (10.0.415.2) SP1 is vulnerable to an out-of-bounds read vulnerability that could allow an attacker to disclose information and execute arbitrary code on affected installations of Cscape.

CVE-2025-4098 has been assigned to this vulnerability. A CVSS v3.1 base score of 7.8 has been calculated; the CVSS vector string is (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H <https://www.first.org/cvss/calculator/3.1#cvss:3.1/av:l/ac:l/pr:n/ui:r/s:u/c:h/i:h/a:h>).

A CVSS v4 score has also been calculated for CVE-2025-4098. A base score of 8.4 has been calculated; the CVSS vector string is (AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N <https://www.first.org/cvss/calculator/4.0#cvss:4.0/av:l/ac:l/at:n/pr:n/ui:a/vc:h/vi:h/va:h/sc:n/si:n/sa:n>).

3.3 BACKGROUND

- **CRITICAL INFRASTRUCTURE SECTORS:** Critical Manufacturing
- **COUNTRIES/AREAS DEPLOYED:** Worldwide
- **COMPANY HEADQUARTERS LOCATION:** United States

3.4 RESEARCHER

Michael Heinzl reported this vulnerability to CISA.

4. MITIGATIONS

Horner Automation has released Cscape version 10.1 SP1 <https://hornerautomation.com/cscape-software-free/cscape-software/> for download.

For more information, see Horner Automation's release notes <https://hornerautomation.com/cscape-software-free/cscape-software/>.

CISA recommends users take defensive measures to minimize the risk of exploitation of this vulnerability, such as:

- Minimize network exposure for all control system devices and/or systems, ensuring they are not accessible from the internet <https://www.cisa.gov/uscert/ics/alerts/ics-alert-10-301-01>.
- 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 <https://www.cisa.gov/resources-tools/resources/ics-recommended-practices> on the ICS webpage on cisa.gov/ics <https://www.cisa.gov/topics/industrial-control-systems>. 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 <https://us-cert.cisa.gov/sites/default/files/recommended_practices/nccic_ics-cert_defense_in_depth_2016_s508c.pdf>.

CISA encourages organizations to implement recommended cybersecurity strategies for proactive defense of ICS assets <https://www.cisa.gov/sites/default/files/publications/cybersecurity_best_practices_for_industrial_control_systems.pdf>.

Additional mitigation guidance and recommended practices are publicly available on the ICS webpage at cisa.gov/ics <https://www.cisa.gov/topics/industrial-control-systems> in the technical information paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies <https://www.cisa.gov/uscert/ics/tips/ics-tip-12-146-01b>.

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

CISA also recommends users take the following measures to protect themselves from social engineering attacks:

- Do not click web links or open attachments in unsolicited email messages.
- Refer to Recognizing and Avoiding Email Scams <https://www.cisa.gov/uscert/sites/default/files/publications/emailscams0905.pdf> for more information on avoiding email scams.
- Refer to Avoiding Social Engineering and Phishing Attacks <https://www.cisa.gov/uscert/ncas/tips/st04-014> for more information on social engineering attacks.

No known public exploitation specifically targeting this vulnerability has been reported to CISA at this time. This vulnerability is not exploitable remotely.

5. UPDATE HISTORY

- May 8, 2025: Initial Publication

This product is provided subject to this Notification </notification> and this Privacy & Use </privacy-policy> policy.

Vendor

- Horner Automation

Tags

Sector: Critical Manufacturing Sector </topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/critical-manufacturing-sector>

Topics: Industrial Control System Vulnerabilities </topics/industrial-control-systems/industrial-control-system-vulnerabilities>, Industrial Control Systems </topics/industrial-control-systems>

Please share your thoughts

We recently updated our anonymous product survey; we'd welcome your feedback.

Related Advisories

MAY 08, 2025 **ICS ADVISORY | ICSA-25-128-02**

Hitachi Energy RTU500 Series </news-events/ics-advisories/icsa-25-128-02>

MAY 08, 2025 **ICS ADVISORY | ICSA-25-128-03**

Mitsubishi Electric CC-Link IE TSN </news-events/ics-advisories/icsa-25-128-03>

MAY 06, 2025 **ICS ADVISORY | ICSA-25-126-03**

BrightSign Players </news-events/ics-advisories/icsa-25-126-03>

MAY 06, 2025 **ICS ADVISORY | ICSA-25-126-01**

Optigo Networks ONS NC600 </news-events/ics-advisories/icsa-25-126-01>

Return to top

Topics </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools>

News & Events </news-events> **Careers** </careers> **About** </about>

CISA Central

1-844-Say-CISA SayCISA@cisa.dhs.gov

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