SA No.: SA-2026-01
Notification Date: September 21, 2026

SECURITY ADVISORY

Unauthenticated Heap Buffer Overflow in Web Administration Interface

Summary

A high-severity heap buffer overflow vulnerability in the web administration interface allows an unauthenticated remote attacker to cause a denial of service and may allow remote code execution. No authentication or user interaction is required.

Issue Description

The web server incorrectly handles excessively large HTTP POST Content-Length values. An integer overflow during buffer size calculation leads to a pre-authentication heap buffer overflow when processing the request body.

Severity

- CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
- CVSS 3.1 Base Score: 8.1 (High)

Affected Products

- All SmartFlex, SmartStart, ICR-2xxx, ICR-3xxx, and ICR-4xxx devices running firmware prior to 6.6.2.
- All ICR-16xx and ICR-17xx devices running firmware prior to 1.6.2.

Solution

- Upgrade affected SmartFlex, SmartStart, ICR-2xxx, ICR-3xxx, and ICR-4xxx devices to firmware version 6.6.2 or later.
- Upgrade affected ICR-16xx and ICR-17xx devices to firmware version 1.6.2 or later.

Acknowledgement

This vulnerability was discovered by Reid Wightman from Dragos.

Related Advisories

CVE-2026-14339

Revision History

2026-09-21 Advisory published

Advantech Czech s.r.o.
Sokolská 71, Kerhartice
562 04 Ústí nad Orlicí
Czech Republic

Tel: +420 465 524 421
E-mail: cellular.info@advantech.cz
Web: www.advantech.cz

IČO: 24148661
DIČ: CZ24148661