

Security Bulletin

20261027: CVE-2026-111497

Security Advisory: Critical Brotli Decompression Vulnerability (Broccoli2Shell)

First published: October 28, 2026. Revision 2.

Summary

Description	A critical vulnerability in the Brotli decompression library, including the copy bundled with Node.js, CVE-2026-111497 (also known as Broccoli2Shell), could allow unauthorized remote code execution on affected systems. DIBT is not aware of any confirmed exploitation affecting Delta products. Delta has updated Building Canvas. Red5-PLUS and O3-Edge r1.0g+ controller firmware includes the affected library; exposure depends on Node-RED, which is disabled by default. Updated firmware is available for 4.21 and 4.19, and an update for 4.18 is pending.
Products	Building Canvas, Red5-PLUS controllers, and O3-Edge r1.0g+ controllers (affected). See Impacted Products.
Recommended Action	No customer action is required for Building Canvas. For Red5-PLUS and O3-Edge r1.0g+ controllers, install firmware 4.21.322 or 4.19.1.3. For Red5-PLUS controllers on 4.18, keep Node-RED disabled unless required and apply the temporary mitigations below until updated firmware is available.

CVE ID	CVSS Vector	Score
CVE-2026-111497	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N	9.2 Critical

Impacted Products

Category	Products
Software and cloud services	Building Canvas
Controllers	Red5-PLUS (firmware 4.21 before 4.21.322, 4.19 before 4.19.1.3, and 4.18); O3-Edge r1.0g+ (firmware 4.21 before 4.21.322 and 4.19 before 4.19.1.3)

Security Bulletin

Software and Cloud Security Updates

Product	Status	Customer action
Building Canvas	Building Canvas services updated to a patched Node.js release	None required

Controller Security Updates

This vulnerability affects Red5-PLUS and O3-Edge r1.0g+ controller firmware. Updated firmware is available for 4.21 and 4.19, and an update for 4.18 is pending. Install updated firmware as soon as it is practical for your controller and site requirements.

Firmware	Applies to	Status
4.18	Red5-PLUS controllers running 4.18	Pending. More information in the coming days.
4.19.1.3	Red5-PLUS and O3-Edge r1.0g+ controllers running 4.19	Available. Contact your local DIBT partner for download.
4.21.322	Red5-PLUS and O3-Edge r1.0g+ controllers running 4.21	Available. Contact your local DIBT partner for download.

Temporary Mitigation for Red5-PLUS Controllers on 4.18

On Red5-PLUS and O3-Edge r1.0g+ controllers that are not yet updated, exposure depends on Node-RED, which is disabled by default but can be enabled and configured by customers. Flows that process externally supplied compressed data may expose the affected library to attacker-controlled input. Until updated firmware is installed:

- Keep Node-RED disabled unless it is required for the site.
- If Node-RED is enabled, review flows that make HTTP requests or process compressed data from external sources, and remove or restrict any that are not required.
- Keep all IP-based controllers within trusted local networks and protected from unauthorized external access.
- Do not expose controllers directly to the public internet.

Next Steps

DIBT will announce the availability of updated Red5-PLUS firmware for 4.18 when it is ready, and will update this bulletin if its review identifies any additional affected products. Temporary mitigations reduce exposure but are not a substitute for installing security updates. DIBT asks all Delta Partners and customers to review their installations and take the appropriate action for each notice above.