

Security Bulletin

20260817: CVE-2026-109618, CVE-2026-109619

Summary

First published: October 21, 2026

Description	This is a follow-up to our earlier communication on two critical PHP vulnerabilities, CVE-2026-109618 and CVE-2026-109619, that could allow unauthorized remote code execution on affected systems. enteliCLOUD and Canvas are patched and a security patch for enteliWEB is now available. We are not aware of any confirmed exploitation affecting Delta products.	
Products	enteliWEB (patch available for 4.29 and newer; 4.28 and older must upgrade first); enteliCLOUD (patched, no action required); Canvas (patched); All V4 IP-Based Controllers: Red5-PLUS-11xx/6xx, Red5-EDGE-11xx/6xx, Red5-EDGE-Vxxx, Red5-PLUS-ROOM, Red5-EDGE-ROOM, O3-EDGE, O3-SENSE, eBMGR-2 (V4), eBCON-2 (All V4 versions) Patch pending for V4.18 LTS, V4.21 firmware, and 4.19 (O3 products only)	
Recommended Action	Apply the enteliWEB security patch immediately to all installations on 4.29 or newer, and upgrade 4.28 and older to 4.29 or newer before patching . Keep the mitigations below in place until patches are applied to each product. Firmware patches not yet available – further instructions will be provided when available	
CVE ID	CVSS Vector	Score
CVE-2026-109618	CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N	9.2 Critical
CVE-2026-109619	CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N	9.2 Critical

Security Bulletin

Description

Delta Intelligent Building Technologies is aware of two critical vulnerabilities in PHP (CVE-2026-109618 and CVE-2026-109619) that could allow unauthorized remote code execution on affected systems. Patches and mitigations are being rolled out product by product as described below.

Immediate Mitigation Measures

- **1. enteliWEB security patch and unpatched installations**
The enteliWEB security patch is available at <https://support.deltacontrols.com/support/downloads/enteliwebfixes/>. It applies to enteliWEB 4.29 and newer and should be applied immediately. Installations on 4.28 or older must first be upgraded to 4.29 or newer, then patched. Until an installation is patched, all enteliWEB servers must be protected from direct access through the public internet: ensure they are not publicly accessible, review firewall configurations, port forwarding, and other network settings to prevent unauthorized external access, and where remote access is required, use a secure VPN or equivalent protected connection.
- **2. IP Based Red5, eBUS, and O3 controllers**
Disable the embedded HTTPS web server by disabling the HTTPS port using network port object NP20001, then verify the HTTPS service is no longer accessible. Keep this mitigation in place until updated firmware is released.
- **3. IP-based Red5, eBUS, and O3 controllers**
Contain all IP-based controllers within a trusted local IP network and do not expose them directly to the public internet. Block incoming TCP traffic on port 443 to the controllers at the network firewall, and ensure controllers are accessible only through trusted, authorized networks.

After making these changes, confirm that essential building automation communications remain operational, particularly where BACnet Secure Connect (BACnet/SC) is in use.

These mitigations are intended to reduce exposure while permanent fixes are prepared. They are not a substitute for applying security updates once released.

Security Bulletin

Planned Remediation via Upgrade

Status by product:

enteliCLOUD: All instances and the enteliCLOUD Portal have been patched. No action is required from customers.

enteliWEB: Security patch available now for 4.29 and newer. Apply immediately; upgrade 4.28 and older to 4.29 or newer first.

Building Canvas: Canvas Workspace has been patched. No action is required from customers. Keep mitigations in place.

All V4 controller firmware: Security patches in development for 4.18LTS, 4.21, and 4.19 (O3 only). Availability will be announced when ready. Keep controller mitigations in place.

We will continue to provide updates as security patches become available for the remaining affected products. We ask all Delta Partners to review their installations and take the appropriate actions immediately.