

Security Bulletin

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

Security Advisory: Critical PHP Vulnerabilities

First published: October 22, 2026. Revision 3: October 27, 2026.

Summary

Description	Two critical PHP vulnerabilities, CVE-2026-109618 and CVE-2026-109619, could allow unauthorized remote code execution on affected systems. We are not aware of any confirmed exploitation affecting Delta products. Patches and mitigations are rolling out by product as described below.
Products	enteliWEB, enteliCLOUD, Building Canvas, and all V4 IP-based controllers (affected). See Impacted Products.
Recommended Action	Apply the enteliWEB security patch to all installations on 4.29 or newer. Upgrade 4.28 and older to 4.29 or newer, then patch. Apply the controller temporary mitigations until a firmware security update is installed. Install 4.21.0.322 where applicable, and do not install 4.21.0.320.

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

Impacted Products

Category	Products
Software and cloud services	enteliWEB, enteliCLOUD, Building Canvas
V4 IP-based controllers	Red5-PLUS-11xx/6xx, Red5-EDGE-11xx/6xx, Red5-EDGE-Vxxx, Red5-EDGE-Vxxx-T1L, Red5-PLUS-ROOM, Red5-EDGE-ROOM, O3-EDGE, O3-SENSE, eBMGR-2 (V4), eBCON-2 (V4)

Security Bulletin

Software and Cloud Security Updates

Product	Status	Customer action
enteliCLOUD	All instances and the enteliCLOUD Portal patched	None required
Building Canvas	Building Canvas Workspace patched	None required
enteliWEB 4.29 and newer	Security patch available: https://support.deltacontrols.com/support/downloads/enteliwebfixes/	Apply as soon as possible
enteliWEB 4.28 and older	Upgrade required before patching	Contact Technical Support for upgrade guidance, then patch

Required Protection for enteliWEB Servers

All enteliWEB servers must be protected from direct public internet access, including after the patch is applied.

- Ensure enteliWEB servers are not publicly accessible.
- Review firewall rules, port forwarding, and other network settings to prevent unauthorized external access.
- Where remote access is required, use a secure VPN or equivalent protected connection.

Controller Security Updates

These vulnerabilities affect all V4 controller firmware. Apply the appropriate update as soon as it is available for your controller and site requirements.

Firmware	Applies to	Status
4.18.3 LTS	Products running 4.18 or earlier, where supported	Pending. More information in the coming days.
4.19.1.3	O3 products only	Pending. More information in the coming days.
4.21.0.322	V4 IP-based controllers other than O3, where supported	Available. Download: https://support.deltacontrols.com/wp-content/uploads/2026/10/4.21.0.322_OP_delay-PHP_patch.zip

Security Bulletin

4.18.3 LTS also includes the following corrections:

- V4FW-15620 (V4FW-13430): missing embedded web password update page.
- V4FW-15623 (V4FW-15395): SMI motors that do not respond to commands.
- V4FW-16071 (V4FW-15862): delayed Red5 output responses.
- V4FW-16040: BBMD and Accept Foreign Devices settings not carried over when upgrading from V3.40 to V4.18.2.

4.21.0.322 includes the following correction:

- V4FW-15862: Red5 output response issue described in the firmware notice below.

Firmware Issue Notice: Delayed Output Response

Item	Detail
Affected firmware	4.21.0.320
Corrected firmware	4.21.0.322
Affected controllers	Red5-PLUS-I/O, Red5-EDGE-I/O, Red5-FIELD-IO, Red5-PLUS-I/O-SF, Red5-EDGE-I/O-SF, Red5-FIELD-IO-SF

Analog and binary outputs may take several minutes to respond to commands from a controller program or a user, and connected equipment may respond later than intended. Input and output configuration changes may also fail to take effect. The issue may develop after extended operation, so controllers that appear normal may still be affected.

- If planning to upgrade to 4.21.0: install 4.21.0.322. Do not install 4.21.0.320.
- If already running 4.21.0.320: upgrade affected controllers to 4.21.0.322 as soon as possible, even if no symptoms have been observed.
- For LTS sites: continue on the LTS branch where site requirements permit. For compatible non-SF models, 4.18.2.10 LTS remains the recommendation until 4.18.3 LTS is released. Controllers on 4.18.2.10 still require the temporary security measures below until a security update is installed.
- For help selecting firmware, contact Technical Support.

This issue was not detected during initial long-term testing. We are reviewing extended-duration testing to improve detection of problems that emerge over time. We apologize for the disruption.

Temporary Mitigation for Unpatched Controllers

For all V4 IP-based controllers that have not received a security update, the embedded HTTPS web server must be disabled until updated firmware is installed.

Disable the HTTPS port using network port object NP8. For firmware 4.21 and earlier, also disable the out-of-service property in the NP8 object.

- Verify that the HTTPS service is no longer accessible.

Security Bulletin

- Keep all IP-based controllers within trusted local networks and protected from unauthorized external access.
- Do not expose controllers directly to the public internet.
- Ensure the network firewall blocks incoming TCP traffic on port 443 to controllers.
- Review network configurations so 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 used.

Next Steps

We will announce the availability of 4.18.3 LTS and 4.19.1.3 when they are ready. Temporary mitigations reduce exposure but are not a substitute for installing security updates. We ask all Delta Partners and customers to review their installations and take the appropriate action for each notice above.

Support and Contact

Latest bulletins: <https://deltacontrols.com/programs-services/cybersecurity/>