



Dear Partner,

Delta Intelligent Building Technologies is aware of two recently disclosed critical vulnerabilities in PHP (CVE-2026-109618 and CVE-2026-109619) that could allow unauthorized remote code execution on affected systems.

We have successfully patched Building Canvas Workspace, all enteliCLOUD instances. A patch for enteliWEB version 4.29 and newer is now available at:

https://support.deltacontrols.com/support/downloads/enteliwebfixes/

While this vulnerability affects all V4 firmware, we are currently working on a security update for 4.18LTS, 4.19 (O3 only), and 4.21

At this time, we are not aware of any confirmed exploitation affecting Delta Intelligent Building Technologies products. However, given the severity of these vulnerabilities, we strongly recommend that all Delta Partners and customers take the following precautionary measures immediately.

Impacted Products

The following products are impacted by these vulnerabilities:

Software and Cloud Services

- enteliWEB
- enteliCLOUD
- Building Canvas

All 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)

Immediate Mitigation Measures

1. enteliWEB Servers

All enteliWEB servers must be protected from direct access through the public internet.

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

2. IP Based Red5, eBUS, and O3 Controllers

For all V4 IP-based controllers, the embedded HTTPS web server **must be disabled** as a temporary mitigation measure until updated firmware becomes available.

- Disable the HTTPS port using network port object NP20001.
- Verify that the HTTPS service is no longer accessible after making the change.

3. IP-Based Controllers Red5, eBUS, and O3 Controllers

All IP-based controllers must be contained within a trusted local IP network and protected from external access.

- Do not expose any IP based controllers directly to the public internet.
- Ensure **incoming TCP traffic on port 443 is blocked** to the controllers through the network firewall.
- Review network configurations to ensure controllers are accessible only through trusted, authorized networks.

When making these changes, please confirm that essential building automation communications remain operational, particularly where BACnet Secure Connect (BACnet/SC) is being used.

Security Updates

Delta Intelligent Building Technologies is actively addressing these vulnerabilities across the affected products:

- **enteliCLOUD:** All enteliCLOUD instances have now been patched, as well as the enteliCLOUD Portal. No action is required from customers.
- **enteliWEB:** A security patch is now available. Please see https://support.deltacontrols.com/support/downloads/enteliwebfixes/
- **Building Canvas:** The Building Canvas Workspace has been patched. No action is required from customers.
- **V4.18 LTS and V4.21 Controller Firmware:** Security patches are in development for 4.18LTS, 4.19 (O3 only), and 4.21. Availability will be announced when the patches are ready.

We will provide further information regarding the availability and deployment of these security updates as they become available.

The measures outlined above are intended to reduce exposure while permanent fixes are being prepared. **They are not a substitute for applying the security updates once released.**

We ask all Delta Partners to review their installations and take the appropriate actions immediately.

Thank you for your cooperation in helping protect our customers and their building automation systems.

Product Management and Cyber Security Teams

Delta Intelligent Building Technologies

© 2026 Delta Intelligent Building Technologies (Canada) Inc. All Rights Reserved.

Delta Intelligent Building Technologies (Canada) Inc. | 17850 - 56th Avenue | Surrey, BC V3S 1C7 CA

Unsubscribe | Update Profile | Constant Contact Data Notice