

Product Bulletin

Security update advisory for XWEB PRO monitoring systems

Dear Customer,

For over 20 years, Copeland Controls has been a trusted leader in Refrigeration and HVAC, delivering reliable, high-quality products that set industry standards. Our legacy is built on a foundation of excellence, powered by rigorous testing and an unwavering commitment to reliability and performance. Copeland Controls' XWEB monitoring units have provided reliable service to customers across essential markets for over two decades. During that time, technology and security requirements have evolved significantly, and we are committed to ensuring that our products meet today's standards.

Safeguarding the safety, quality, and security of our products is integral to everything we do. We actively partner with the global cybersecurity community, encouraging external experts to report potential vulnerabilities through our dedicated processes. This fosters transparency, trust, and continuous improvement.

We recently discovered vulnerabilities with the XWEB PRO monitoring units. A comprehensive investigation was launched, deploying all necessary fixes swiftly to address the vulnerabilities and ensure our customers' systems remain secure.

The firmware version 1.13 addresses and provides mitigation for all previously identified security vulnerabilities.

Any new vulnerabilities identified will be addressed in subsequent release.

We strongly encourage you to deploy all the updated firmware.

See our website below for updates:

For the latest firmware: <https://webapps.copeland.com/Dixell/Pages/SystemSoftwareUpdate>

Email Technical Support: dixell.service@copeland.com

FAQ

Question: Have these vulnerabilities been exploited?

Answer: No, there have been no reports of exploitation. This is a proactive disclosure.

Question: What devices are impacted?

Answer: All XWEB PRO models exposed to the Internet.

Question: What should I do right now?

Answer:

1. Ensure your devices are not exposed to the public Internet and begin planning for firmware updates once released;
2. Restrict access to physical equipment to authorized personnel only (e.g. restrict personnel, keyed entry where possible);
3. Follow Copeland Controls' recommendations to adhere to all instructions and specifications included with the device manual and following security best practices, including but not limited to:
 - never exposing the control system to the broader Internet;
 - configuring your firewall to restrict access to administrative protocols, like SSH;
 - configuring your network to restrict inbound and outbound communications to and from the control system;
 - ensuring default account passwords are updated and all passwords align with industry best practices;
 - configuring and enabling HTTPS for web-based traffic but not exposing the controller's web interface to the broader Internet.