



MANUFACTURERS OF COMPUTERIZED TEMPERATURE CONTROL FOR FORTY-SIX YEARS

PROUDLY MADE IN FULTON, MISSOURI, USA

A certified "Service Disabled Veteran Owned Small Business" (SDVOSB)

2105 Power Lane, Fulton, Missouri 65251

October 21, 2026

**MEMORANDUM
IMMEDIATE RELEASE**

From: Ben Trout III, President
To: All Customers, Information Technology

--- ORIGINAL MEMORANDUM BELOW THIS UPDATE ---

--- **UPDATE 1: October 21, 2026 1:51 PM** ---

PHP has released a patch for the PHP security vulnerabilities CVE-2026-109618 and CVE-2026-109619. The patches will be released for PHP versions 8.2, 8.3, 8.4, 8.5. Patches for versions before this will NOT be published as those versions are beyond PHP's END OF LIFE.

Before this vulnerability was announced, we offered all of our customers the ability to update their core SBD-3200 operating system with the current release, which also automatically updated all of the dependencies (such as the PHP version). If you are one of the systems that took advantage of this opportunity, then you have a version of the PHP core that can be updated. We are implementing a remote patch operation at this time. If this operation is successful, we will patch all of the updates we recently performed.

If however, you still have an older SBD-3200, it will have to be sent into us to have it's core operating system updated. This will include the patch. As before, we will perform these updates at minimal cost, but you will need to call for availability and pricing. We have never forced our customers to upgrade anything, and we're not going to start now.

Please review the original memo below for more complete information.

Ben Trout III

www.epmctc.com

Fulton, Mo. (573) 642-6550 / Fax (573) 642-6556 Wichita, Ks. (316) 269-2660
Service (573) 642-6550

--- ORIGINAL MEMORANDUM October 21, 2026 7:30 AM ---

We are aware of the PHP security vulnerability, and are working to determine it's scope as it pertains to your SBD-3200 network appliance.

AT THIS TIME, we believe this to be limited in severity to that of a minor inconvenience.

As always, the most severe breach of the SBD-3200 that could ever be exposed, is a ROOT level FULLY AUTHENTICATED access to the core command prompt with ELEVATED PERMISSIONS. At that point, an attacker would still be limited to the temperature control interface computer. IF an attacker then configured the appliance, using tools that are not natively installed, and attempted to "reach out" to the rest of your network, your own network security would come into play. We cannot answer to this architecture, as we don't even know the extent of that.

The SBD-3200 contains no sensitive information about our customers, or even nodes on your network. At most, an attacker determines the temperature history in one of your rooms, or even deletes the software that provides the human interface to your system.

The firmware that actually operates the facility runs on a separate machine, and that code is burned into a chip. This cannot be modified in-place.

In 1986, our systems were Y2K compliant. Your faith in our company will never be mis-placed.

We will make further announcements when appropriate.

