

Critical PHP Vulnerabilities in macmon and NRSW

Date: 2026-10-22

Version: 1.0

Summary

CVE-2026-109619: PHP has various global state that temporarily points into request memory. In some scenarios, global state may not be correctly reset, or may be repopulated after being reset. The global state may then refer to request memory even after it has been freed. Subsequent requests may read or branch on this stale state before it is fully initialized. Multiple strategies can trigger this condition and produce remote code execution (RCE).

CVE-2026-109618: PHP uses longjmp() for out-of-memory (OOM) errors to exit the current context and abort handling of the request. Some contexts may not properly account for this scenario and leave request memory in an uninitialized state before performing an allocation. The subsequent request cleanup procedure may read or branch on this memory. Multiple OOM strategies can consistently trigger this condition and lead to remote code execution (RCE).

The following vulnerability affects one or more versions of the products listed in the next section:

ID	Title / Description	Severity
CVE-2026-109619	Remote code execution in PHP	CVSS v3.1: 9.8
CVE-2026-109618	Remote code execution in PHP	CVSS v3.1: 9.8

Affected Products

Brand	Product Line	Affected Version(s)
NetModule	NRSW	All
macmon	macmon	6.x/7.x

Mitigation

NRSW:

All NRSW versions are affected by the latest PHP vulnerabilities (CVE-2026-109618 / 109619), including the latest mainline release 5.0.0.104.

The mitigation steps we recommend until we publish a release with the patched vulnerabilities is to disable the web-interface after making sure there is a ssh connection to the device, by issuing these commands:

```
cli-set http.status=0
cli-set https.status=0
```

macmon:

The macmon version 6.x and 7.x are both using PHP in for the web UI and are therefore affected by the latest PHP vulnerabilities (CVE-2026-109618 / 109619).

As mitigation the web UI (HTTPS/443) **must not** be accessible from the Internet without protection. Access to the interface and guest portal should be restricted to trusted networks whenever possible.

This applies for version 7.x **until** the patch is applied, and for version 6.x permanently until upgrading to 7.x. It is strongly recommended updating to the current 7.x version and install the patch, which can be downloaded from the [service portal](#).

For Help or Feedback

To view all Belden Security Advisories or to report suspected security vulnerabilities, go to <https://www.belden.com/security>.

For technical support and other requests, please visit <https://www.belden.com/support/technical-product-support-main>.

Related Links

- [NVD-CVE-2026-109619](#)
- [NVD-CVE-2026-109618](#)

Disclaimer

THE SECURITY ADVISORY, AND INFORMATION CONTAINED HEREIN, ARE PROVIDED ON AN "AS IS" BASIS AND DO NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE ADVISORY, AND INFORMATION CONTAINED HEREIN, OR MATERIALS LINKED FROM THE ADVISORY, IS AT YOUR OWN RISK. INFORMATION IN THIS ADVISORY AND ANY RELATED COMMUNICATIONS IS BASED ON OUR KNOWLEDGE AT THE TIME OF PUBLICATION AND IS SUBJECT TO CHANGE WITHOUT NOTICE. BELDEN RESERVES THE RIGHT TO CHANGE OR UPDATE ADVISORIES AT ANY TIME.

Revisions

V1.0 2026-10-22 Security Advisory published.