

PHP runtime vulnerability.

Vulnerability: Remote code execution in the bundled PHP runtime (CVE-2026-109618, CVE-2026-109619)

Severity: Critical (CVSS 9.2)

Components affected: ICT WebClient, ICT ArmorIP

Reported by: Erik Hamilton

Active exploitation of vulnerability*: No

Description of vulnerability: Two vulnerabilities in the PHP runtime bundled with the affected products allow a remote, unauthenticated attacker to execute arbitrary code - and, for CVE-2026-109619, potentially read sensitive in-process memory - by sending specially crafted HTTP requests to the web interface. The flaws are in the PHP runtime, not in ICT code.

Affected versions: WebClient up to and including 1.48.3.1; ArmorIP up to and including 3.0.18.2

Mitigation: Upgrade to the fixed release - WebClient 1.48.4.0 or ArmorIP 3.0.18.3 - which bundle the patched PHP runtime. Upgrading is the only complete fix. Where immediate upgrade is not possible, restrict the web interface to trusted networks; the interim PHP settings `session.upload_progress.enabled=0` (all affected versions) and `fatal_error_backtraces=0` (PHP 8.5 only) reduce but do not remove the risk.

References: CVE-2026-109618, CVE-2026-109619; PHP advisories GHSA-w8hw-w9fx-j79w, GHSA-6wmf-4rv5-p3rp

*This indicates whether ICT is aware of this being actively exploited against customer sites at the time of publication.