



Hardcat PHP2Shell Vulnerability: Assessment

Shannon Binch

V1.1 23 October, 2026

1 Document Control

1.1 Document Details

Project	Hardcat
Title	Hardcat PHP Vulnerability Assessment
Document Status	Final

1.2 Document Revision History

Date	Version	Author	Change Description
22/10/2026	0.1	Shannon Binch	Created
22/10/2026	1.0	Damien Gallagher	Reviewed, approved
23/10/2026	1.1	Shannon Binch	Updated

1.3 Reference Documents

Document	Version	Author

Information (CVE-2026-109618, CVE-2026-109619)

Hardcat does not use PHP within its internal network or software environment and is therefore not affected by this vulnerability internally.

However, PHP is used on the externally hosted Hardcat.com website, which is hosted separately from and isolated from our internal network and systems.

Hardcat has not identified any indicators of compromise or evidence that this vulnerability has been exploited on the Hardcat website. At this stage, there is no indication that the vulnerability has been used to gain unauthorized access or negatively impact the website's operation.

We have been advised by our hosting provider that they will implement the necessary remediation once an official patch becomes available. Given the current assessment and the absence of any evidence of exploitation, there is no need to take the website offline at this time.

The website primarily contains public marketing and informational content and does not store financial information or other sensitive customer data. The Hardcat website is not used to transact client data, client representative information. Nor is the site used for financial transactions. As an additional precaution, Hardcat will continue to monitor the environment for any signs of suspicious activity and will ensure that patching is completed in accordance with our security management processes once a suitable update is released.