

Attempts to Exploit Critical PHP Server Vulnerabilities

This advisory is relevant to all Tongan individuals, businesses and institutions. It is intended to be understood by both general and technical audiences. Individuals, businesses and institutions are encouraged to remain aware of phishing activity and consider the available measures outlined below. These measures can help reduce the likelihood of phishing emails being successful, particularly where emails may appear legitimate or familiar.

What’s happened?

Two critical PHP vulnerabilities disclosed on 21 October 2026 could allow unauthorised attackers to take control of internet-facing PHP servers. The issue affects all supported PHP branches, public exploit code is available, and active exploitation has already been reported. There is no effective workaround other than applying the vendor patches. Businesses using PHP-based web services should treat this as an urgent patching priority, particularly where systems are internet-facing or running unsupported versions. The following are notable impacts.

- 

Unauthorised remote code execution on internet-facing PHP Servers
- 

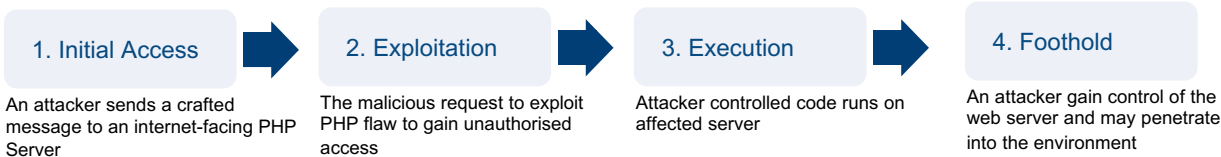
Stealing sensitive personal/corporate data
- 

Bypassing Application Defences
- 

Higher exposure when using End-of-Life PHP Versions
- 

Creates opportunity for large-scale attack

What does the attack pathway look like?



What can we learn from this?

These observations provide an opportunity to strengthen awareness and help protect individuals, businesses, institutions and the communities they serve across Tonga.

Threat Mitigations

Mitigating Controls: *Steps that can help reduce the likelihood of PHP vulnerability exploitation*

- 1. Apply Patches:** Where practical, apply patches to all PHP servers immediately to the latest fixed version, while prioritising internet-facing servers.
- 2. Vendor Recommendation.** Where patching cannot be applied immediately, apply temporary vendor-recommended safeguards, noting these do not fully remove the risk.
- 3. Enhance Monitoring:** Where possible, Increase monitoring for unusual web requests, PHP errors, suspicious worker behaviour, and unexpected outbound connections.
- 4. Threat Hunting.** Consider conducting targeted threat hunting to identify signs of exploitation or post-compromise activity, such as web shells or abnormal server processes.

Where can I go for help?

If you have received or responded to a phishing email, or would like assistance or advice, you can contact CERT Tonga directly at the contact details provided.



CERT Tonga Ministry of MEIDECC Nuku'alofa
Tel: 2378 (CERT) | Email: cert@cert.gov.to |
Web: <https://cert.gov.to/> | Twitter: @CERTTonga
| Facebook: @CERTTonga

TLP: CLEAR