UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00128

PHP PROJECT INFILTRATED BY ATTACKERS

DATE ISSUED: 6th April 2021

OVERVIEW

The discovery of two malicious commits, including a backdoor in the PHP scripting language Git repository server has sparked an investigation as to how attackers were able to gain access.

BREAKDOWN

PHP is a commonly and widely used web-application scripting language that has the capability to be embedded into HTML and this week those responsible for the maintenance of the php-src repository caught the malicious code before it went into production. It appeared the attackers were preparing for a supply-chain style of attack that would allow them access to all the websites their scripts had compromised. Evidence suggests that this was potentially more than compromised credentials, as the commits were uploaded using the names of the maintainers. In response to the breach, PHP are moving their servers to GitHub and combing through the libraries to locate any other potential security threats or further corruption.

REMEDIATION STEPS

- As the breach was caught before it went live, no action is required.

REFERENCES & RESOURCES

Tech Republic https://www.techrepublic.com/article/php-programming-language-source-code-targeted-in-backdoor-attack/
Bleeping Computer https://www.bleepingcomputer.com/news/security/phps-git-server-hacked-to-add-backdoors-to-php-source-code/
We Live Security https://www.welivesecurity.com/2021/03/30/backdoor-php-source-code-git-server-breach/
Threatpost https://threatpost.com/php-infiltrated-backdoor-malware/165061/