ADVISORY REPORT ON PHP Git repository hack
Advisory report on PHP Git repository hack

Date: 26th April 2021
Problem ID & Name: PHP Git Repository Hack
Severity: Medium

Executive Summary

A suspicious threat actor compromised the popular server-side language PHP’s git repository. It is believed that the attacker committed a couple of changes to its source code repository that had a backdoor and allowed a Remote Code Execution (RCE) the maintainers of the project revealed. PHP is a widely used server-side programming language and almost used by 80% of the websites. So far, the intentions of the attackers is unknown and upon investigating this in depth it came into light that the commits were made under the names of legitimate members.

Digging deeper into the issue, it was found that the code created a backdoor that allowed attackers to take control over any website that used PHP remotely. In a statement released by one of the chief maintainers, the attackers have found a way to hack the server on which the repository was hosted. He further added PHP is investigating into the repositories for the matters of corruption beyond the couple of recently made commits. Since this attack did not cause the carnage as expected, we categorise it under medium severity.
As per the mitigation and recommendation

As a mitigation step for the future, the maintainers have decided not to accept any commits on the main server. However, the changes can be made on GitHub. Both the commits are fix a typo of commits according to the maintainers.

The amendments to the code were first spotted by the contributors and one of them revealed that a particular line of code executes from a user HTTP header if the string begins with zerodium. It is one of the leading companies that buys zero-day exploits.

As you can see in the above screenshot where the backdoor is implemented and the threat actors can gain the access remotely/ In addition to this the chief maintainer of the repository said, they are going to implement MFA after the attack, making sure this is not repeated in the future.
References

1) https://portswigger.net/daily-swig/backdoor-planted-in-php-git-repository-after-server-hack
3) https://www.welivesecurity.com/2021/03/30/backdoor-php-source-code-git-server-breach/

Revision Table:

<table>
<thead>
<tr>
<th>SI. NO.</th>
<th>DESCRIPTION</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Initial Public Release</td>
<td>Final</td>
</tr>
</tbody>
</table>

Issued by

Research wing: CyberPeace Foundation

Research Wing, Autobot Infosec Private Ltd.