金融資安資訊分享與分析中心

弱點公告-1081101

(PHP 7 遠端程式碼執行漏洞**)**

發行日期：2019 年 11 月 1 日

TLP:WHITE

PHP 7 漏洞資訊

〔TLP：WHITE〕

資料來源及時間： NIST， 2019/10/28

摘要:

PHP 7 存在漏洞，可利用此漏洞取得受影響設備的控制權。

概述:

PHP 7.1.x 低於 7.1.33、7.2.X 低於 7.2.24 和 7.3.X 低於 7.3.11 的版本中 FPM (FastCGI Process Manager)設定的某些組態，可能會導致 FPM 模組將先前分配的緩衝區資料寫入到為 FCGI 協議資料保留的空間中，從而導致可遠端執行程式碼。

使用 NGINX 伺服器且啟用了 PHP-FPM 始存在此漏洞可供利用。

目前此漏洞已經出現攻擊程式碼，請參考 https://www.exploit-db.com/exploits/47553 及 https://github.com/neex/phuip-fpizdam

影響平台

PHP 且使用 NGINX 平台

7.1.X:小於 7.1.33 版本

7.2.X:小於 7.2.24 版本

7.3.X:小於 7.3.11 版本

因應對策 or 建議措施

TLP:WHITE

建議測試完成後，升級至原廠建議版本。

CVSS 向量:

使用版本：CVSS 3.1

分析分數：9.8

分析向量：AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

資料來源：NIST NVD

參考連結：

1. NVD CVE-2019-11043

   https://nvd.nist.gov/vuln/detail/CVE-2019-11043

2. CIS

   https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-php-could-allow-for-arbitrary-code-execution_2019-116/

3. ZDNet

   https://www.zdnet.com/article/nasty-php7-remote-code-execution-bug-exploited-in-the-wild/