



## ThinkPHP Remote Code Execution Vulnerability

### Open source PHP framework vulnerabilities still being exploited in the wild

<https://blog.thinkphp.cn/869075>

CVEs: [CVE-2019-9082](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9082), [CVE-2018-20062](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20062)

A remote code execution vulnerability exists within multiple subsystems of ThinkPHP 5.0.x and 5.1.x. The FortiGuard Labs continue seeing high exploitation attempts of these old vulnerabilities of more than 50,000 IPS device detections per day. There are multiple actors abusing this flaw to install malware such as Mirai like botnet, Lucifer, Cryptocurrency miners.

#### Background

ThinkPHP is a free framework distributed under the Apache2 open-source license primarily used for Web application development and simplifying enterprise application development. Both the CVE-2019-9082 and CVE-2018-20062 are on CISA's list of known exploited vulnerabilities (KEV) added in the year 2021 and successful exploitation of the flaws could allow a remote attacker to execute arbitrary code on the affected system.

#### Announced

Dec 10, 2018: CVE-2018-20062, flaw discovered in noneCMS ThinkPHP.

<https://github.com/nangge/noneCms/issues/21>

Jan 11, 2019: CVE-2019-9082, flaw discovered in ThinkPHP package.

[https://github.com/suitablecodes/open\\_source\\_bms/issues/33](https://github.com/suitablecodes/open_source_bms/issues/33)

Nov 03, 2021: CVE-2019-9082 and CVE-2018-20062, added to CISA's known exploited list.

#### Latest Developments

FortiGuard customers remain protected by the IPS signature which was first released in 2018 and last updated in 2021. With IPS detections still at large in 2023 and online exploit availability for the CVEs, FortiGuard labs recommends users to immediately review and upgrade the vulnerable version of ThinkPHP to 5.0.23 / 5.1.31 and above.

## PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

#### Reconnaissance

##### Decoy VM

Detects and blocks lateral movement on the network segment



FortiDeceptor

v3.3+

#### Weaponization

##### AV

Detects and blocks malware related to vulnerability (CVE-2019-9082, CVE-2018-20062)



FortiWeb

DB 9.0.2485



FortiClient

DB 9.0.2485



FortiSASE

DB 9.0.2485



FortiMail

DB 9.0.2485



FortiCASB

DB 9.0.2485



FortiCWP

DB 9.0.2485

##### FortiProxy

DB 9.0.2485

##### AV (Pre-filter)

Detects and blocks malware related to vulnerability (CVE-2019-9082, CVE-2018-20062)



FortiEDR

DB 9.0.2485



FortiSandbox

DB 9.0.2485

#### Behavior Detection

AI detection engine detects and blocks other 0day malware, unkown threats, and rates known malware related to ThinkPHP RCE as "High risk".



FortiSandbox

v4.0+

#### Exploitation

##### IPS

Detects and blocks attempts to exploit the vulnerability (CVE-2019-9082, CVE-2018-20062)



FortiGate

DB 18.1.41



FortiSASE

DB 18.1.41



FortiNDR

DB 18.1.41



FortiADC

DB 18.1.41



FortiProxy

DB 18.1.41

#### Web App Security

Detects and blocks attempts to exploit the vulnerability (CVE-2019-9082)



FortiWeb

DB 0.00347



FortiADC

DB 1.00042

#### Installation

##### Post-execution

Detects and blocks post-exploitation activity related to zero day vulnerabilities and unknown malware



FortiEDR

v5.0+

#### C2

#### Action

## DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

#### Threat Hunting



FortiEDR

v5.0+



FortiAnalyzer

v6.4+



FortiSIEM

v6.6+

#### Outbreak Detection



FortiAnalyzer

DB 1.00098

#### Content Update



FortiSIEM

v304

#### FortiSIEM

## RESPOND

Develop containment techniques to mitigate impacts of security events:

#### Automated Response

Services that can automatically respond to this outbreak.



FortiXDR

v1.0.0042

#### Assisted Response Services

Experts to assist you with analysis, containment and response activities.



FortiResponse



FortiACI

#### RECOVER

## RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

#### InfoSec Services

Security readiness and awareness training for SOC teams, InfoSec and general employees.



FortiResponse

v1.0.0042

#### IDENTIFY

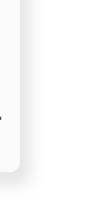
Identify processes and assets that need protection:

#### Attack Surface Monitoring (Inside & Outside)

Security reconnaissance and penetration testing services, covering both internal & external attack vectors, including those introduced internally via software supply chain.



FortiRating



FortiRecon



FortiDAST

#### Additional Resources

##### ThinkPHP

<https://github.com/top-think>

##### Threatpost

<https://threatpost.com/self-propagating-lucifer-malware-targets-windows-systems/156883/>

Learn more about [FortiGuard Outbreak Alerts](#)

