



NOTICE · UPDATED LIVE

PHP2SHELL: CRITICAL PHP VULNERABILITY, UPDATE TODAY AT 16:00 CEST

Today at 16:00 CEST, PHP is releasing an emergency update for two critical security vulnerabilities. As a precaution, we are taking the websites and applications we manage offline until that update has been installed and tested. Here you can read what is going on, what we are doing and what it means for you.

Client sites temporarily offline

LAST UPDATED WEDNESDAY 21 OCTOBER AT 16:34

UPDATES

NEWEST FIRST

16 hours ago · 16:33

RESOLVED, ALL SERVICES BACK ONLINE

Within 38 minutes of the fix being released, all systems we manage have been updated, checked and brought back online. We also reviewed for any suspicious activity and found none. If your service is reachable again, the flaw has been closed.

WHAT ARE YOU RUNNING INTO?

CLOSE

Write down what is going on. You get an answer from a developer within one working day, not from a form robot.

Your name

Email address

Phone (optional)

What is it about?

SEND →

RATHER CALL? +31 10 307 00 33

As a precaution, we are taking the websites and applications we manage offline until the 16:00 CEST update has been installed and tested. You do not need to do anything. We will let you know as soon as your site is back online.

yesterday · 08:30

BEVEILIGINGSLEK IN PHP BEKENDGEMAAKT

A serious security flaw in PHP was disclosed today, known as PHP2Shell. PHP is the technology that many websites and web applications run on. The official fix is due this afternoon at 16:00 CEST. Because the information leaked early, we are acting today and will keep you updated here.

WHAT ARE YOU RUNNING INTO?

Write down what is going on. You get an answer from a developer within one working day, not from a form robot.

→

RATHER CALL? +31 10 307 00 33

reports, it is triggered while processing forms and uploads, which PHP does before any website code runs. A security plugin, Laravel or WordPress will not stop it.

Until the update is out, no measure fully closes the hole. So we are taking the safest route: the websites and applications we manage go offline until the update has been installed and tested. We would rather be unreachable for a few hours than run a server someone else can get into.

03

WHAT WE DO FROM 16:00

WHAT ARE YOU RUNNING INTO?

Write down what is going on. You get an answer from a developer within one working day, not from a form robot.

→

RATHER CALL? +31 10 307 00 33

WHAT ARE YOU RUNNING INTO?

Write down what is going on. You get an answer from a developer within one working day, not from a form robot.

→

RATHER CALL? +31 10 307 00 33



Until 16:00, PHP has only confirmed that there are two critical vulnerabilities, how severe they are and when the update is coming. Which versions are affected and how the vulnerability works will be published by PHP at 16:00. What is written above about the cause comes from researchers' reports and may turn out differently. We will update this page as soon as more is known.



FREQUENTLY ASKED QUESTIONS

WHAT ARE YOU RUNNING INTO?

Write down what is going on. You get an answer from a developer within one working day, not from a form robot.

→

RATHER CALL? +31 10 307 00 33



SERGE HUIJSEN
Founder, developer

Questions? Call or email us. We are on it today.

Call +31 10 318 0515

info@codeiq.nl

WHAT ARE YOU RUNNING INTO?

Write down what is going on. You get an answer from a developer within one working day, not from a form robot.

→

RATHER CALL? +31 10 307 00 33



Hoge Filterweg 314
3063 KG Rotterdam

+31 10 318 0515
info@codeiq.nl

CoC 91812003 · VAT NL865779247B01

WHAT WE DO

INDUSTRIES

WHAT ARE YOU RUNNING INTO?

Write down what is going on. You get an answer from a developer within one working day, not from a form robot.

→

RATHER CALL? +31 10 307 00 33

© 2026 CODEIQ. CODEIQ IS A TRADE NAME OF
SHWEB B.V.

[PRIVACY POLICY](#)

[TERMS AND CONDITIONS](#)

[DATA BREACH PROTOCOL](#)

[NL](#) [EN](#)