MCP Server Security Incident

by Robert Meyer | Nov 07, 2026



What is happening, what we know and how we deal with it. We have had a security incident. We've found out how the attacker did it, and we want you to know what we're doing. So here's what happened when and what does it mean today? One thing in advance: The mStudio is available again. You can log in again now. We successfully locked out the attackers.

In the shadow of PHP2Shell

On the evening of 21.10., the whole IT world was busy with PHP2Shell. It is precisely at this time that the attacker tests a vulnerability in our MCP server for the first time. From 23.10. he will be a regular user on our platform. It registers test accounts, uses extensions, and performs simple injection attempts.
On October 27 at 2:58 p.m., he registers another account, with which he exploits the vulnerability found in the MCP server at 3:03 p.m. In our logs, we can see that he works his way through our system extremely quickly. This points to the use of AI tools. In some cases, only seconds pass between steps, which would have to take much longer with a human attacker.
In our logs, we can also see that the attacker disguises his accesses and performs various distraction maneuvers, which we will focus on initially.
After analyzing this timeline, it was clear to us: We treat all data as of 10/27 as compromised.

What has happened since the discovery

Wednesday, 11/4: Detection and containment
On the morning of 11/4, we discovered unusual behavior in one of our systems. At 11:11 a.m., we blocke attacker's first account. After that, things went from strength to strength: Extensive analyses by interna experts began, and gradually other relevant specialists were activated. The extent was unclear u a feel for the scope at 12:53 p.m. and set the status page to "Investigation".

As a precautionary measure, we are taking parts of our systems offline. We use the time to prevent further access and to revoke access. We can identify the MCP server as a gateway and shut it down.

Beratungsteam
Hallo 👋 Schön, dass du da bist! Du schreibst direkt mit unserem Produktberatungsteam – mit echten Menschen statt einem Bot. Wir helfen dir gerne dabei, den passenden Tarif zu finden.

In the evening, the mStudio will be online again. The web projects were available throughout.

Thursday, 11/5: Continuing to clean up and secure
After we blocked projects in which traces of the attacker could be found shortly after midnight, we have also temporarily disabled the registration of new accounts. During the course of the day, we will block the login to the mStudio and access to the customer projects via SSH.
External IT forensic experts support us on an ongoing basis in the analysis. We have informed the responsible authorities.

Friday, 6.11.: Hardening and processing
We have forensically evaluated 56 compromised projects and the MCP server. After repeated scans of our systems, we did not find any more compromised projects. We are currently unable to prove any activity by an attacker on our systems. The mStudio can be used again during the night.

Saturday, 7.11.: Activation and Passkeys
The mStudio is available again and can be used again. We have also reactivated the SSH accesses in this context. The websites we blocked as a precaution will remain blocked for the time being. If further measures are necessary, we will inform affected customers again by e-mail.
Since the question reached us via various channels: The customer center and the websites managed in it were not affected by the security incident at any time.
With the activation of the mStudio, you can now also set up a passkey.

vServer – Der Agenturliebling

Top Performance für viele Projekte

Jetzt buchen

What happens now

First the PHP2Shell vulnerability, now the attack on our systems: AI attacks will occur more frequently in the future. We want to be transparent about this, so we will publish a detailed account of the events next week once our analysis and recovery is fully completed. We will deal with this throughout the weekend and beyond. You will receive relevant information from us proactively via the status page and by e-mail. If we find that other customers are affected and need to act, we will inform them personally and accompany them in the necessary steps.

To the FAQs

Robert Meyer

Robert Meyer is the founder and managing director of Mittwald. More than 20 years ago, he laid the foundation for the company – since then, the service character and the attributes "love of agencies, reliability and sustainability" have been his top priorities in relation to Mittwald.



Related articles: