

A series of supercomputers in Europe were suddenly attacked

The number of supercomputers affected in this incident amounted to more than 12.

Several high-performance computers (HPC) and data centers used for major research projects across Europe were forced to shut down last week due to cyber security issues. surprise.

The number of supercomputers affected in this incident amounted to more than 12, concentrated mainly in Germany, England and Switzerland, making it impossible for researchers to continue their work, and the original damage estimated. Count is not small. Supercomputers are extremely powerful systems built on high-performance hardware to perform large computations in a short period of time. They are used primarily in science and testing mathematical models involving complicated physical phenomena and designs.

Many supercomputers stopped working at the same time

Earlier this week, a series of announcements began from the United States and Germany related to information that European supercomputers were forced to shut down after a relatively large-scale mysterious cyberattack operation. and complicated.

In the UK

ARCHER, the British national supercomputer service, has started to 'cover' since 11 May due to the successful exploitation of a security flaw on its login nodes. External access to this supercomputer service is currently locked without any notice of when it will resume. The password and SSH key will be reset, meaning that the user will log in when the online service comes back, they will need to provide 2 login credentials: the SSH key and the new ARCHER password.



ARCHER supercomputer

In Germany

On the same day, May 11, the Baden-Württemberg (bwHPC) project in Germany also announced the existence of a security incident that made five of its servers unavailable. The exact time when the activity resumed.

A similar situation happened with the Leibniz Supercomputer Center, which involved a security incident that left its high-performance computers numb and administrators forced to shut down the entire system for maintenance.

The German Jülich Supercomputer Center (JSC) announced on May 14 that their JURECA, JUDA and JUWELS supercomputers are no longer available due to IT security incidents.

Over the weekend, at least nine supercomputers in Germany were affected by cyber attacks, according to SPIEGEL journalist Patrick Beuth.

In Switzerland

The BwForCluster NEMO supercomputer in Freiburg, Switzerland, commonly used to study neuroscience, particle physics and microsystems, has also been hacked. A total of 7 attacks were recorded, the first of which took place on January 9.

On May 16, the Swiss Center for Scientific Calculations (CSCS) also issued a notice saying that some high-performance computers and academic data centers are no longer accessible because Administrators discover malicious activity exists on the system.

Attacks supercomputer on a large scale

In the latest report of the European Grid Infrastructure (EGI), the attacker used the SSH credentials they obtained to hack from server to server with the purpose of abusing CPU resources to Mining cryptocurrency Monero. Some servers are used for exploitation, others act as proxies to connect to the exploit server.

The Computer Security Incident Response Team (CSIRT) at EGI found that in some cases, malicious exploits were configured to run only during the hours and nights, in order to avoid being detected.

At the moment, there is not much information about the attack campaign, but it does not exclude the possibility that this campaign was carried out by a large hacker organization, targeting cryptocurrencies and even spreading. spreading malware (malware). Investigation and restoration of the operation of the affected supercomputers is being urgently deployed.

You finished reading the article "**A series of supercomputers in Europe were suddenly attacked**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.