

# WEEKLY BULLETIN

## 27-31 JANUARY 2024



Quote

"It takes 20 years to build a reputation and minutes of a cyber incident to ruin it."

Stephane Nappo

of the week

Content:

- Workshop: "A safer space for children"
- Fintech - data breach
- Ivanti - patching alert



### Workshop: "A safer space for children"

In the framework of "A safer cyber space for children", NAECCS coordinates the work with the State Agency for the Rights and Protection of Children (ASHMDF), in a Workshop with the same topic. Also organized in cooperation with the City Hall, the activity was organized on January 31, 2024, in the city of Durrës.

The workshop was developed within the framework of raising awareness among children and young people about a safer cyber space, bringing to attention on the one hand the positive contributions of the development of technology, but on the other hand awareness of the many risks they can face in cases of inappropriate use of digital space.

Children and parents should know that for any concern encountered in various forms such as: psychological violence, abuse, neglect, etc., they can report to the official website of NAECCS on the "Report inappropriate content" platform, or they can notify the ASHMDF and the line helpers for children, Alo 116 111. Participants in this workshop were representatives from local government, law enforcement institutions, social workers, children of different age groups from 9-year-old and secondary schools, teachers, parents, as well as representatives of non-governmental organizations that play an important role for the protection of children.



### Fintech - data breach

Direct Trading Technologies, an international fintech company, jeopardized over 300K traders by leaking their sensitive data and trading activity, thereby putting them at risk of an account takeover.

The leaked data includes the commercial activity of over 300,000 users over the past six years, along with names, email addresses, emails sent by the company and IP addresses.

Although the problem was fixed, the company has not yet issued an official response.

[Read more](#)

## PATCHING ALERT



### Ivanti - patching alert

Ivanti has recently warned of two new vulnerabilities rated critical in its Connect Secure and Policy Secure products, one of which has been actively exploited.

As a workaround to address the vulnerabilities identified as: CVE-2024-21888 and CVE-2024-21893, users are recommended to import the "mitigation.release.20240126.5.xml" file.

[Read more](#)