

WEEKLY BULLETIN

5-9 JUN 2023



Quote

"Cybersecurity isn't something you buy, it's something you make, and it takes talented people to do it right."

of the week

Content:

- Albania, the first in the regional cyber security exercise organized as a friendly competition format!
- Microsoft OneDrive shuts down worldwide after claims of DDoS attacks
- Honda- data breach
- Google Chrome-Patching Alert



Vulnerabilities in the Honda eCommerce Platform could expose customer data

Cybersecurity researchers have discovered serious vulnerabilities in a Honda e-commerce platform used for sales of various marine, energy, equipment etc. The attackers could have gained access to more than 21,000 customer orders ranging from 2016 to 2023, including name, address, phone number and information on the items ordered. The vulnerabilities also exposed 1,500 merchant pages that could have been modified by the attacker. After these problems were reported, the Japanese firm confirmed that all problems had been fixed.

[Read more](#)

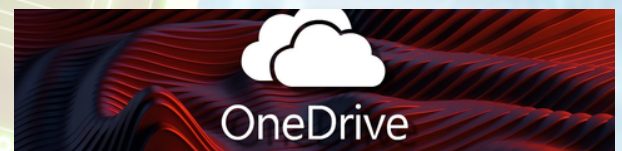
PATCHING ALERT



Zero-Day alert: Google releases an update for a new vulnerability

Google released security updates to patch a serious vulnerability in its Chrome web browser that was being actively exploited. Identified as CVE-2023-3079, the vulnerability allows an attacker to potentially exploit a large amount of data via a crafted HTML page. Users are recommended to update Chrome version 114.0.5735.110 for Windows and 114.0.5735.106 for macOS and Linux to mitigate potential threats. AKCESK recommends all Google Chrome users to install the latest updates.

[Read more](#)



Microsoft OneDrive shuts down worldwide after claims of DDoS attacks

Microsoft is currently investigating an ongoing service outage that prevents customers from using Cloud services around the world. While the company did not provide any details on what is causing the outage, attackers identified as "Anonymous Sudan" claim to have attacked Microsoft OneDrive services through DDoS attacks. Microsoft Teams said they are investigating the incident and are taking the necessary steps to protect customers and ensure the stability of their services.

[Read more](#)



Albania, the first in the regional cyber security exercise organized as a friendly competition format!

The 4-day cyber training, organized by the Estonian eGovernance Academy, CybExer Technologies, the National Information Society Agency (AKSHI), the National Authority for Electronic Certification and Cyber Security (AKCESK) and other competent security authorities, with the support of the European Union, was held in Tirana where cyber security experts from Albania, Montenegro, and North Macedonia participated. The Albanian team, led by representatives of AKSHI and AKCESK, with participants from other security institutions and critical information infrastructures, showed excellent skills in responding to a cyber attack simulation, ranking first.

The activity was attended by the President of the Republic of Albania H.E.S. Bajram Begaj together with the President of the Republic of Estonia, H.E.S. Alar Karis and the Ambassador of the European Union H.S. Mrs. Christiane Hohmann.

General Director of AKCESK, Mr. Igli Tafa, in his speech, thanked the European Union, the Estonian President, and the Academy of Electronic Government of Estonia for their continued support, underlining that by working together we can protect our countries and our citizens from cyber threats and create a future where our infrastructures are safe and sustainable.

The General Director of AKSHI, Mrs. Mirlinda Karçanaj, during this activity, first thanked the EU ambassador in Tirana, who made it possible to organize this activity, the European and American partners who are supporting Albania, and praised the work of AKCESK for setting standards and raising awareness in the field of cyber security, with the help of the eGovernance Academy, which has provided support in the drafting of the legal framework as well as consulting on the management of cyber security in the private sector. Ms. Karcanaj underlined that after the sophisticated attack on Albania last year sponsored by a state not friendly to our country, these simulations are important for increasing the skills of our experts.

At a time when cyber security challenges are global, Albania has increased its focus on increasing technical capacities for responsible cyber security staff. AKCESK continues working intensively to strengthen cooperation and increase the level of cyber security by implementing the best international practices and expertise.