WEEKLY BULLETIN
21-25 AUGUST 2023

Quote of the week

"Even the bravest cyber defense will experience defeat when weaknesses are neglected."

Stephane Nappo

Content:

A new vulnerability is discovered in WinRAR

A security vulnerability rated as critical has been discovered in the WinRAR program that could potentially be exploited by a threat actor to achieve remote code execution on Windows systems.Successful exploitation of the vulnerability requires interaction with the user by tricking them into visiting a malicious page or simply opening an infectious file.

Users are recommended to update to the latest version of WinRAR to mitigate potential threats.

Read more

Google Workspace will require two admins to sign off on critical changes.

Google announced today new cybersecurity defense controls that will allow security teams to thwart social engineering attacks like phishing targeting Workspace users and prevent account takeover attempts.

Google also explained how Android malware can slip into the Google Play Store with the help of a tactic known as versioning that enables malicious actors to evade the store's review process and security controls.

Read more

60 Million Individuals Impacted by MOVEit Hack

Nearly 1,000 organizations and 60 million individuals are reported to have been affected by the latest MOVEit campaign carried out by the Russian hacking group ClOP.

ClOp, which is estimated to have earned up to $100 million as a result of this campaign, has begun extracting the data of victims who have refused to pay.

Read more

PATCHING ALERT

Cisco Patches High-Severity Vulnerabilities in Enterprise Applications

Cisco announced recentely security updates for several enterprise applications to patch high-severity vulnerabilities leading to privilege escalation, SQL injection, directory traversal, and denial-of-service (DoS).

Cisco says it is not aware of any of these vulnerabilities being exploited in malicious attacks. However, users are advised to update their installations as soon as possible, as known vulnerabilities in Cisco appliances are often exploited in the wild.

Read more

Rruga "Papa Gjon Pali II", No.3
info@cesk.gov.al
Autoriteti Kombëtar për CESK
autoriteti_kombetar_cesk
+35542221039