

BULETIN JAVOR

21-25 GUSHT 2023



Shprehja

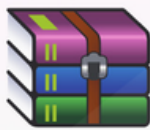
"Edhe mbrojtja kibernetike më e hekurt do të përjetojë humbje kur dobësitë neglizhohen."

Stephane Nappo

e javës

Përmbajtja:

- Zbulohet një vulnerabilitet i ri në WinRAR
- 60 milionë individë të prekur nga hakimi i MOVEit
- Google Workspace kërkon identifikimin e dy administratorëve gjatë ndryshimeve kritike.
- Cisco - Patching Alert



WinRAR®

Zbulohet një vulnerabilitet i ri në WinRAR

Një vulnerabilitet sigurie e vlerësuar si kritike është zbuluar në programin WinRAR ku mund të shfrytëzohet potencialisht nga një aktor kërcënimi për të arritur ekzekutimin e kodit në distancë në sistemet Windows.

Shfrytëzimi i suksesshëm i vulnerabilitetit kërkon ndërveprim me përdoruesin duke e manipuluar të vizitohet një faqe keqdashëse ose thjesht duke hapur një skedar infektues.

Përdoruesve u rekomandohet të përditësojnë versionin më të fundit të WinRAR për të zbutur kërcënimet e mundshme.

[Link: Lexo më shumë](#)



Google Workspace kërkon identifikimin e dy administratorëve gjatë ndryshimeve kritike.

Google njoftoi së fundmi kontrollin të reja të mbrojtjes së sigurisë kibernetike që do të lejojnë ekipet e sigurisë të pengojnë sulmet e inxhinierisë sociale të cilat synojnë përdoruesit e Workspace.

Google shpjegoi gjithashtu se si një malware Androidi mund të infektojë Google Play Store me ndihmën e një taktike të njohur si versionimi që u mundëson aktorëve keqdashës të shmangin kontrollin e sigurisë.

[Lexo më shumë](#)



60 milionë individë të prekur nga hakimi i MOVEit

Gati 1000 organizata dhe 60 milionë individë raportohet se janë prekur nga fushata e fundit MOVEit e kryer nga grupi sulmues rus CI0P.

CI0p, e cila vlerësohet të ketë fituar deri në 100 milionë dollarë si rezultat i kësaj fushate, ka filluar të nxjerrë të dhënat e viktimave që kanë refuzuar të kryejnë pagesën.

[Link: Lexo më shumë](#)

PATCHING ALERT



Cisco përditëson vulnerabilitete me severitet të lartë në aplikacionet Enterprise.

Cisco lancoi përditësimet e sigurisë për disa aplikacione Enterprise për të korrigjuar vulnerabilitetet kritike që lejojnë përshkallëzimin e privilegjeve, injektimin SQL, kalimin dhe mohimin e shërbimit (DoS).

Cisco njoftoi se nuk është në dijeni të ndonjë prej këtyre vulnerabiliteteve të shfrytëzohet nga sulmuesit. Megjithatë, përdoruesit këshillohen që të përditësojnë instalimet e tyre sa më shpejt të jetë e mundur, pasi vulnerabilitetet e njohura në pajisjet Cisco shpesh shfrytëzohen aktivisht.

[Link: Lexo më shumë](#)