

Iknedēļas ziņas
Sagatavotas 14.03.2016.
Numurs 2016/10

Kontakti: prese@cert.lv
Tālrunis: 67085888

Web aplikācija ļauj piekļūt lietotāja datiem

Kāda sociālā tīkla web aplikācijā tika konstatēta iespēja nesankcionēti iegūt lietotāju identifikācijas datus (vārdu, uzvārdu, attēlu), meklējot pēc telefona numura, ja lietotājs to bija reģistrējis sociālajā tīklā. Meklējamajai personai pat nav jābūt meklētāja draugu lokā, lai tās numuru uzrādītu. Lietotnes uzturētāji tika brīdināti par ievainojamību.

Informācijas noplūde pakalpojuma pieteikumu formā

Kādā sakaru operatora lapā, piesakot pakalpojumus vai veicot iepirkumus, tika nekorekti apstrādāti dažu sesiju dati. Lapas apmeklētājam tika atgriezta informācija par kādu citu portāla lietotāju un tā veiktajiem pasūtījumiem. Šie dati saturēja arī pilna apjoma lietotāja identifikācijas informāciju, ieskaitot personas kodu un tālruna numuru. Šī kļūda novērota tikai epizodiski. Pakalpojuma uzturētāji tika brīdināti.

Mēģinājums atklāt ievainojamības

Pret kādas pašvaldības pakalpojumu sniedzēju lapu ar automātisku ielaušanās rīku tika veikti ielaušanās mēģinājumi. Uzbrucējam neizdevās kompromitēt lapu. Pakalpojumu sniedzējs tika informēts.

Krāpnieciska lapa piedāvā jūrnieku sertifikātus

Tika atklāts, ka kāda mājas lapa uzdodas par kompāniju, kas it kā izsniedz jūrnieku sertifikātus. Lapa lūdz interesentus iesniegt nepieciešamo informāciju sertifikāta saņemšanai, ieskaitot personas datus. Lapa satur viltus informāciju un nelikumīgi izmanto Latvijas Jūras spēku flotiles ģerboni. Pēc izpētes secināts, ka šāda kompānija nepastāv un nav sertificēta izsniegt jūrnieku sertifikātus. CERT.LV ir informējis šīs vietnes uzturētājus, kā arī lapas uzturētājvalsts CERT komandu, lai novērstu šīs vietnes turpmāku darbību.

Nozog naudu no Facebook piesaistītās kredītkartes

Kādam uzņēmumam tika kompromitēts Facebook konts, un no tam piesaistītās kredītkartes tika nozagti apmēram 2000 EUR. Ar šo naudu tika veikta no uzņēmuma nepieprasītu reklāmu apmaksas. Pēc Facebook un kredītkartes izdevējbankas informēšanas, nauda tika atgūta. CERT.LV iesaka reklāmu apmaksai izmantot speciālu karti, bez kredītlimita un ar nelielu konta atlikumu.

Vīrusi arhivētos dokumentos

Viltus rēķinu veidā tiek izsūtīti .ace formāta arhīva pielikumi, kas satur KAZY saimes trojas vīrusu.

Plašāka informācija par vīrusu: <https://msisac.cisecurity.org/whitepaper/documents/11.pdf>

E-pasta paraugs:

-----Original Message-----
From: Trading Dept
Sent: Monday, March 7, 2016 11:45 AM
Subject: Order List

Dear Sir,

See attached document the list of order for March 2016,Any questions, please feel free to contact us.

Thank You
Mrs Samira
Purchase Dept

> 1 attachment: IPO #824257.ace size unknown