Iknedēļas ziņas
Sagatavotas 29.09.2016.
Numurs 2016/36

## *Pateicoties atbildīgu ievainojamību atklāšanas praksei, izdodas novērst kritiskas ievainojamības*

IT drošības speciālists Nils Putniņš sadarbībā ar uzņēmumu "Influent Solutions" un "Digital Security Alliance" biedrību informēja CERT.LV par atklātu kritisku ievainojamību kādas pašvaldības tīmekļa vietnē. Izmantojot ievainojamību, bija iespējams nesankcionēti iegūt datu bāzes ierakstus un potenciāli pārņemt serveri uzbrucēja kontrolē. Ievainojamības atklāšanā tika ievēroti atbildīgas ievainojamību atklāšanas (responsible disclosure) pamatprincipi un apdraudējumu izdevās operatīvi novērst.

Lai popularizētu atbildīgu ievainojamību atklāšanas praksi, CERT.LV savā tīmekļa vietnē publicēja vadlīnijas atbildīgu ievainojamību atklāšanai CERT.LV publiski pieejamajos servisos.
Vairāk: https://cert.lv/lv/par-mums/atbildiga-ievainojamibu-atklasana

## *Notikuši mērķēti kiberuzbrukumi valsts iestādes darbiniekiem*

Kādā valsts iestādē vairāki darbinieki saņēma savu kolēģu vārdā nosūtītus e-pastus ar virsrakstu "Latvijas Stabilitātes programma 2016.-2019.gadam", kas tika izsūtīti no inbox.lv servera. To pielikums saturēja Microsoft Office formāta dokumentu ar makro funkciju, kas lejupielādēja un izpildīja datorvīrusu. Datoru inficēšana iestādē nav konstatēta.
Ir pamats domāt, ka uzbrucēji bijuši no Korejas.

## *Skolnieks labo atzīmes e-klase.lv portālā*

Tika konstatēts, ka kāds vidusskolas skolnieks labojis savas un klasesbiedru atzīmes e-klase.lv portālā, izmantojot skolotājas paroli. Parole tika iegūta no LinkedIn kompromitēto paroļu datiem, kas ir brīvi pieejami internetā. Nodarījums netieši atgādina, ka parolēm dažādās vietnēs ir jābūt atšķirīgām, citādi tās var viegli piemeklēt.

## *Izķēmots pašvaldības iestādes portāls*

21.09. tika konstatēts, ka izķēmots pašvaldības iestādes portāls. Pēc CERT.LV brīdinājuma iestāde veica pārbaudi, kurā atklāja izķēmošanas cēloni - CMS TikiWiki 14.0 ievainojamību. Portāls tika salabots un tā darbība atjaunota.

## *Kritisku ievainojamību labojums Apple produktiem*

20.09. Adobe izlaida labojumus MacOS Server, MacOS Sierra, Safari, un iCloud for Windows. Dažas no ievainojamībām ļauj iegūt attālinātu kontroli pār upura datoru.
Lietotājiem jāveic programmatūras atjaunināšana.

### *Kritisku ievainojamību labojums Drupal satura vadības sistēmai*

Drupal satura vadības sistēma ir populāra arī Latvijā un to lieto vairāki simti tīmekļa vietņu. 21.09. Drupal 8.x versijām, kas vecākas par 8.1.10 atklātas ievainojamības, no kurām viena ļauj uzbrucējiem iegūt attālinātu kontroli pār upura datoru.