Iknedēļas ziņas
Sagatavotas 22.01.2016.
Numurs 2016/3

Kontakti: prese@cert.lv
Tālrunis: 67085888

Internet Explorer ievainojamība

Atklāta jauna ievainojamība, kas skar Internet Explorer versijas no 8 – 11. Šīs versijas ir pakļautas attālinātai operatīvās atmiņas izmainīšanas ievainojamībai. Ievainojamība ļauj izpildīt kaitīgu kodu, piemēram, lietotājam apmeklējot kādu īpaši tam pielāgotu vietni.
Pagājušajā nedēļā informējām, ka Microsoft pārtrauc atbalsta sniegšanu Internet Explorer versijām, kas vecākas par 11. versiju. Labojumi šai ievainojamībai nav pieejami tām versijām, kurām vairs netiek sniegts Microsoft atbalsts.
Plašāka informācija: https://www.symantec.com/security_response/vulnerability.jsp?bid=76194

Mājas lapa piedzīvo DDoS uzbrukumu

Kāda mājas lapa piedzīvojusi DDoS uzbrukumu no vienas IP adreses, kas mērķējusi pieprasījumus uz konkrētu ievainojamu PHP failu, kā rezultāta pārslogoja tīmekļa serveri. Visdrīzāk uzbrukums bijis sekmīgs dēļ nedroši konfigurētas satura vadības sistēmas WordPress.
Cietušās lapas uzturētāji lūdza CERT.LV palīdzību, lai noskaidrotu no kurienes šis uzbrukums ir nācis un tā iespējamos iemeslus. Turpinās incidenta izmeklēšana.

Jāuzmanās ar MS Office dokumentu atvēršanu

Atkārtoti saņemti macro vīrusa paraugi, kas izveidoti ar mērķi inficēt datorlietotājus ar Dridex bankas trojāni. Šī uzbrukuma kampaņa gan nav izdevusies, jo faili, kuriem jābūt inficētiem, ir bojāti un nav datoram kaitīgi.
CERT.LV iesaka kritiski izvērtēt jebkādu aizdomīgu pielikumu atvēršanu un gadījumos, kad tiek atvērti Microsoft Office dokumenti, izvairīties no macro funkcionalitātes atļaušanas. Microsoft Office programmatūra noklusētā konfigurācijā lietotāju brīdina par macro funkciju esamību un nepieļauj to automātisku izpildi.

Pret pašvaldību vērsts pikšķerēšanas uzbrukums

Kāda novada pašvaldības iestādes darbinieki masveidā saņēmuši pikšķerēšanas e-pastus.
E -pasts aicināja darbiniekus apstiprināt e-pasta adresi un nosūtīt savus personas datus.
CERT.LV rīcībā nav informācijas, ka kāds pašvaldības darbinieks atbildējis uz šo pieprasījumu.

Krāpnieciskā e-pasta paraugs:

```
*Cienījamais deputāts.
Sakarā ar sastrēgumu visu pasta kontu lietotājiem un likvidēt visus neizmantoto
interneta kontiem mēs būsim spiesti slēgt savu kontu, jums ir, lai apstiprinātu
savu e-pastu un aizpildot zemāk savu pieteikšanās informāciju, ja veidlapa nav
pilnībā aizpildīta jūsu konts tiks apturēta 24 stundu drošības apsvērumu dēļ laikā.


Aizpildiet zemāk, datus par jums un apstipriniet
Jūsu dati

Nom:.....................................................................
Vārds
:.....................................................................
Displejs vārdu savā pasta kontu: ..........................................
.........................................
Adrese
mail:.....................................................................
Parole: .........................................
.................................................. ...
Nodarbošanās: ..........................................
.........................................
Valsts: .........................................
.....................................
NB: Visi šie lauki ir obligāti tāpēc, lūdzu, aizpildiet tos.
Šī informācija tiks izmantota, lai nodrošinātu Jūs ar individuālu pieeju.
Paldies un veiksmi.*
```

Ievainojamība Linux kodolā

Atklāta nopietna Linux kodola ievainojamība. Ietekmētas ir Linux operētājsistēmas ar Linux kodolu 3.8 un jaunākas. Šī ievainojamība ietekmē arī Android versijas KitKat un jaunākas.

Ievainojamība uzbrucējam ļauj iegūt "root" lietotāja tiesības. Tas iespējams, palaižot ļaunprātīgu Android vai Linux lietotni kompromitētā iekārtā, vai iekārtā uz kuras uzbrucējam jau ir piekļuve ar nepriviliģētu lietotāju.

Plašāka informācija: http://perception-point.io/2016/01/14/analysis-and-exploitation-of-a-linux-kernel-vulnerability-cve-2016-0728/

Drupal satura vadības sistēmas ievainojamība

Šī gada 6. janvārī tika paziņots par vairākām Drupal satura vadības sistēmas problēmām, kas var tikt izmantotas nesankcionētai koda izpildei un datubāzes piekļuves datu zādzībai. Ievainojamības atrodamas Drupal satura vadības sistēmas atjauninājumu procesā.

Plašāka informācija: https://threatpost.com/all-drupal-versions-susceptible-to-code-execution-credential-theft-vulnerabilities/115802/

Ievainojamību skaidrojums, ietekme un labojumi: https://groups.drupal.org/node/506128

OpenSSH ievainojamība

Šī gada 11. janvārī tika atklāta OpenSSH ievainojamība. Pie noteiktiem apstākļiem izmantojot šo ievainojamību, iespējams iegūt klienta privāto atslēgu. Ievainojamas ir OpenSSH versijas no 5.4 līdz 7.1, veicot pieslēgumu pie kompromitētas iekārtas. Ievainojamības labojums ir jau pieejams. Plašāka informācija: http://www.openssh.com/txt/release-7.1p2