Iknedēļas ziņas
Sagatavotas 29.07.2016.
Numurs 2016/28

Kontakti: prese@cert.lv
Tālrunis: 67085888

Kritiskas ievainojamības LastPass tiešsaistes paroļu pārvaldniekā

Atklātas kritiskas ievainojamības tiešsaistes paroļu pārvaldniekā LastPass, kas ļauj ļaundabīgai lapai attālināti pārņemt kontroli pār lietotāja LastPass kontu. Ievainojamības atklātas drošības pārbaudē Google ProjectZero ietvaros. Šobrīd ļaundabīga ievainojamību izmantošana nav konstatēta.

Ievainojamības viedās apgaismes produktos

Atklātas 9 ievainojamības OSRAM viedās apgaismes kontroles produktos, daļa ievainojamību nav izlabota. Izmantojot atklātās ievainojamības, iespējams pat attālināti piekļūt mājas datortīklam.
Vairāk informācijas: https://community.rapid7.com/community/infosec/blog/2016/07/26/r7-2016-10-multiple-osram-sylvania-osram-lightify-vulnerabilities-cve-2016-5051-through-5059

Krievijas drošības dienestu informācijas operācijas

Publicēts izsmeļošs apkopojums par divām paralēlām kiberoperācijām pret ASV Demokrātu partijas biroju. Pēc drošības kompāniju ziņojumu publicēšanas veikta informācijas operācija – izveidots konts hakerim, kas it kā esot vienatnē uzlauzis demokrātu partiju, kā arī publicēta, iespējams sagrozīta informācija vietnē WikiLeaks.org
Vairāk lasiet: https://motherboard.vice.com/read/all-signs-point-to-russia-being-behind-the-dnc-hack

Kritiskas ievainojamības Xen

Xen virtualizācijā sistēmas kods (privileged, ring 0) spēj izkļūt no virtuālās mašīnas (guest) un izpildīties reālajā mašīnā (host). Ievainojamība (CVE-2016-6258) atklāta visās Xen versijās. Tā veiksmīgi izmantojama uz x86 procesoriem pie zināmiem nosacījumiem, lietojot paravirtualizāciju (PV). Izlaisti atjauninājumi, kas novērš ievainojamību.
Vairāk informācijas: https://xenbits.xen.org/xsa/advisory-182.html

Java ļaunatūra veiksmīgi uzbrūk MacOS

Adwind - platformneatkarīga ļaunatūra, kas rakstīta Java, spēj inficēt MacOS datorus.
Vairāk: https://blog.malwarebytes.com/threat-analysis/2016/07/cross-platform-malware-adwind-infects-mac/

Bezvadu klaviatūru ievainojamība

Atklāts, ka ievainojamības vairākos bezvadu klaviatūru modeļos ļauj pārtvert un piekļūt rakstītajam no ievērojama attāluma (~100m).
Vairāk: https://threatpost.com/keysniffer-vulnerability-opens-wireless-keyboards-to-snooping/119461/

Iesaka atteikties no SMS daudzpakāpju autentifikācijas

ASV Nacionālais standartu un tehnoloģijas institūts (NIST) informē, ka pakalpojamu nodrošinātājiem vajadzētu ņemt vērā, ka atsevišķos gadījumos divu faktoru autentifikācija, izmantojot sms, ir nedroša.
NIST paziņojums:
https://threatpost.com/nist-recommends-sms-two-factor-authentication-deprecation/119507/

Windows ievainojamība ļauj izpildīt ļaundabīgu kodu

Atklāta ievainojamība, ar ko var apiet Windows User Account Controls (UAC) un izpildīt ļaundabīgu kodu.
Vairāk: https://threatpost.com/windows-uac-bypass-leaves-systems-open-to-malicious-dlls/119468/