Viso pasaulio IT specialistus ant kojų sukėlė vadinamoji nulinės dienos kritinė saugumo spraga, pavadinta „Log4Shell“. Ji aptikta plačiai naudojamoje „Apache Log4j“ įrašų bibliotekoje ir kelia pavojų serveriams, duomenų centrams, debesijos bei kitoms paslaugoms. „Telia“ Saugos komandos vadovės Odetos Baranauskienės teigimu, spraga paveikė ir Lietuvos IT paslaugų tiekėjus.

„Log4Shell“ tapo nemalonia staigmena visiems, dirbantiems IT ir saugumo srityje, įskaitant ir mus. Paveikta daug technologijų, sistemų ir visa tai kelia didelę riziką. „Telia“ specialistai ėmėsi skubių veiksmų, diegė naujinimus, bendradarbiaujame su tiekėjais“, – sako O. Baranauskienė.

„Log4Shell“ spragos oficialusis pavadinimas yra CVE-2021-44228. Ji ypač pavojinga dėl to, kad „Log4j“ įrašų biblioteka yra itin populiari – dažniausiai ji sutinkama serverių ir debesijos paslaugų programinėje įrangoje, tačiau tam tikras „Log4j“ variantas gali būti įtrauktas ir į kitas paslaugas, pavyzdžiui, įmonės naudojamą specialiai jai sukurtą programą

Atradę sistemas, kuriose ši spraga dar nėra ištaisyta, piktavaliai gali ja pasinaudoti vykdydami nuotolines komandas ar užvaldydami pačius serverius.

Pasaulyje užfiksuota šimtai tūkstančių bandymų pasinaudoti naująja spraga. Sėkmės atveju programišiai serveriuose įdiegia kriptovaliutų kasimo robotus, kenkėjus DDoS atakoms vykdyti, taip pat užfiksuota bandymų įdiegti išpirkos reikalaujančius virusus.

Interneto forumuose vieša informacija apie kritinę spragą pirmą kartą pasirodė gruodžio 9 dieną, tačiau IT saugumo tyrėjai nustatė, kad programišiai ją aptiko dar gruodžio 1-ąją.

„Didieji paslaugų tiekėjai spragą suskubo ištaisyti, tačiau kadangi „Log4Shell“ spraga yra visiškai šviežia, yra daugybė technologijų, kurios tebėra pažeidžiamos. Ypatingą dėmesį reikėtų atkreipti smulkiam ir vidutiniam verslui, nesvarbu, kokiomis paslaugomis jie naudojasi – rekomenduojame kreiptis į partnerius, prižiūrinčius programinę įrangą su klausimais dėl pažeidžiamumo ir atnaujinimų, nukreipti savo specialistus domėtis nuolat atnaujinama informacija“, – pabrėžia „Telia“ ekspertė.

Ji priduria, kad neužtenka tik įdiegti naujausią „Log4j“ versiją . IT specialistai turėtų papildomai peržiūrėti žurnalinius įrašus ir atlikti kitus sistemos patikrinimus, kurie leistų įvertinti, ar į ją nebuvo įsilaužta ir ar nėra kenkėjiškos veiklos požymių.

Daugiau informacijos apie „Log4Shell“ spragą ir patarimų, kokius veiksmus reikėtų atlikti, rasite Nacionalinio kibernetinio saugumo centro svetainėje.