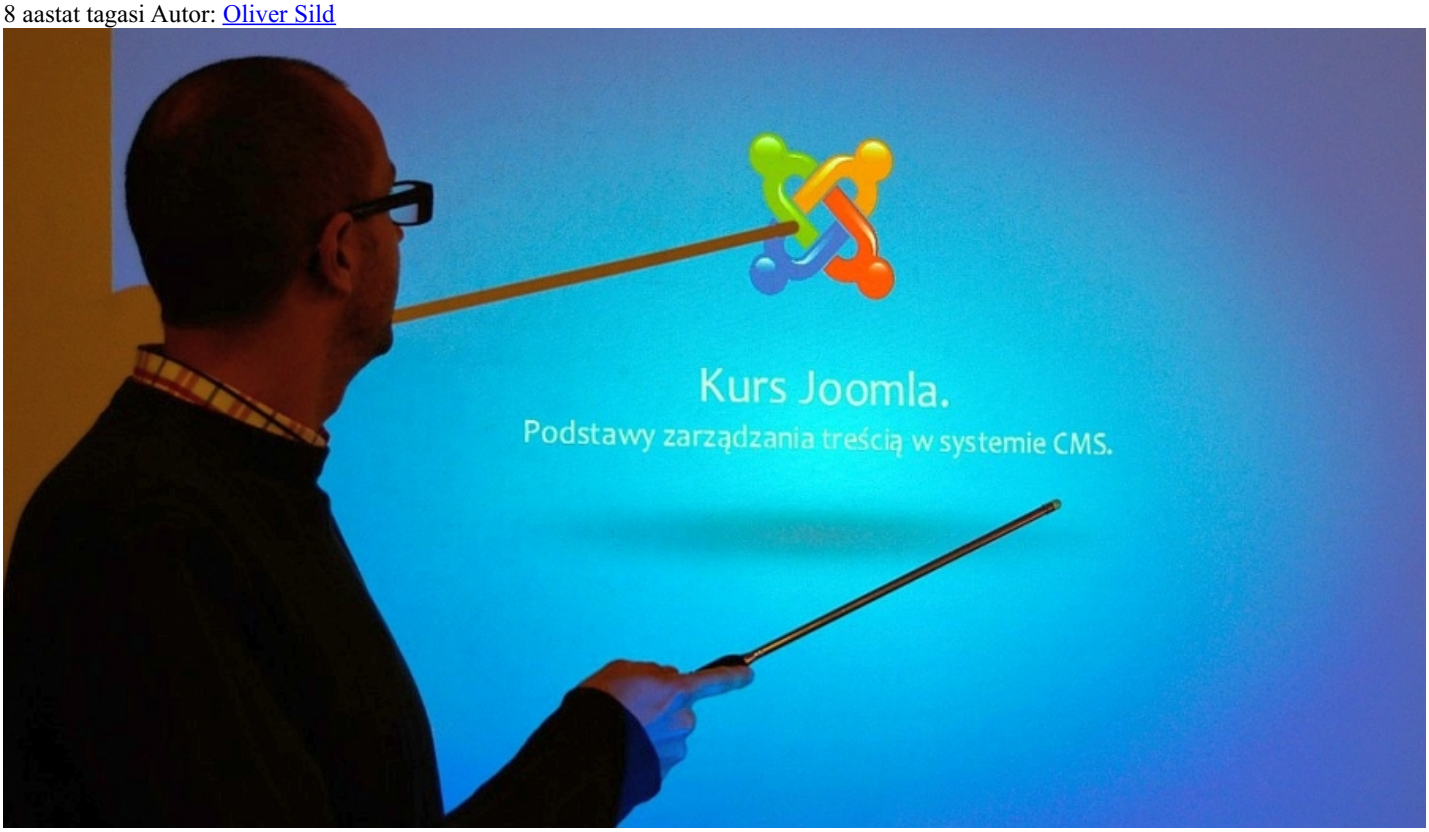
Joomlat rünnatakse - toimub massiline uuendamata veebilehtede langemine

8 aastat tagasi Autor: Oliver Sild



Joomla! on sisuhaldussüsteem, mis jääb populaarsuselt vaid Wordpressist maha. See veebiplatvorm väljastas 25. oktoobril uue versiooni 3.6.4, mis parandab kaks kõrge riskiga haavatavust. Paraku on suur osa veebe veel uuendamata ning nüüd on käes nende turvaaukude ärakasutamise aeg.

Esimest turvariski on võimalik ründajal enda jaoks ära kasutada, et luua uuendamata veebilehele uus kasutaja isegi juhul, kui registreerimine on suletud (vt CVE-2016-8870). Teine haavatavus toetab esimest ning lubab kasutaja õiguseid nö kõrgemaks muuta (vt CVE-2016-8869).

Antud haavatavused mõjutavad miljoneid Joomla! sisuhaldussüsteemil arendatud veebilehti, mis on ikka veel versiooninumbriga 3.4.4 - 3.6.3.

Antud rünnaku läbiviimisel on võimalik veebilehele paigaldada tagauks ning seejärel tagada täielik ligipääs haavatavale lehele. Tihtipeale lisatakse rünnaku käigus veebi ka erinevaid skripte, mis levitavad nii spämmi kui pahavara ning paljudel juhtudel ei pruugi kodulehe omanik oma saidi vastu toimunud rünnakust isegi teadlik olla.

Rünnakuid viiakse läbi massiliselt

Viimastel päevadel on esimese suurema rünnaku läbi tuhandetele veebilehtedele lisatud kasutajaid nimega "db_cfg". Täheldatud on ka Lätist läbi viidud rünnakut, kus samuti mitmetel tuhandatel Joomla! veebilehtel lisati pealtnäha suvaliste kasutajanimedega libakasutajaid. Kuna haavatavus on tehtud avalikuks - nüüdseks on veebis levimas ka skriptid, mis ründaja eest töö ära teevad - siis saab automaatselt haavatavatele veebilehtedele tagauksi paigaldada.

Kui 26. oktoobril suudeti tuvastada 590 rünnakut, mis antud haavatavusi kasutasid, siis 28. oktoobriks on tõusnud ohvrite arv 28 000 juurde. Võib arvata, et tänaseks on see number veelkord mitmekordistunud.

Mida teha?

Kõige lihtsam ja loogilisem on loomulikult kohe uuendada oma Joomla! tarkvara versioon uusima peale, kus turvaaugud on parandatud. Kui kardad, et veebilehe kujundus võib peale uuendamist tuksi minna, siis kasuta tulemüüri ning viirusetõrjega turvamoodulit. Kui ise ei oska antud probleemiga midagi peale hakata, siis kirjuta oma veebilehe arendajale või näiteks Eesti veebiturvalisuse agentuurile (esec.ee).

- Uudised

- Tarkvara
- Turvalisus