Tartu Ülikool
Loodus- ja täppisteaduste valdkond
Arvutiteaduse instituut

Joosep Näks

CVE-2020-4049

Referaat

LTAT.06.002 Andmeturve

Õppejõud: Meelis Roos

2021

Sisukord

1 Sissejuhatus

WordPress on vabavaraline blogihaldamise keskkond, kus saab blogi illustreerimiseks ka üles laadida blogi teemasid, mis muudavad seda, kuidas blogi välja näeb. Turvaauk CVE-2020-4049 on haavatavus teema faili üleslaadimisel, mis laseb teema failinime sisse peita JavaScripti skripti.[1]

Käesolevaga luban Tartu Ülikoolil seda referaati avalikult eksponeerida kuni aastani 2026.

2 Turvaaugu kirjeldus

Turvaauk laseb kasutajal laadida üles teema fail, mille nimesse on peidetud JavaScripti kood, ning seda koodi jooksutatakse blogi teema valimise lehel administraatori õigustega. Turvaaugu risk on madal, kuna ka teema üleslaadimiseks on vaja administraatori õigusi.[2]

3 Ohtlikkus

Üks võimalus turvaaugu ära kasutamiseks oleks see, kui ründaja veenaks psüholoogilise ründe abil blogi administraatorit üles laadima ründaja poolt koostatud ohtliku nimega teema faili ning seejärel kui ükskõik milline blogi administraator avab teemade lehe, käivitub ründaja loodud skript. Selle oht on siiski väike, kuna terve ründaja skript peab olema faili nime sees ehk blogi administraatoril on lihtne märgata, et tegu on kahtlase teema failiga.

4 Parandus

Turvaauk on parandatud alates WordPressi versioonist 5.4.2. Paranduseks tehtud muudatus on järgnev:[3]

Teema faili sisselugemisse lisati funktsioon `esc_html()`, mis leiab sisendist `HTML` sildid üles ning muudab nad selliseks, et `HTML` koodi parsimisel loetaks neid tavalise tekstina. [4] See tähendab et teema faili nimes olevat skripti esitatakse tavatekstine ning see ei käivitu enam blogi teemade lehe avamisel.

Viited

[1] `https://nvd.nist.gov/vuln/detail/CVE-2020-4049#vulnCurrentDescriptionTitle`

[2] Turvaaugu meililist: `https://lists.debian.org/debian-lts-announce/2020/07/msg00000.html`

[3] Parandus githubis: `https://github.com/WordPress/wordpress-develop/commit/404f397b4012fd9d382e55bf7d206c1317f01148`

[4] `https://developer.wordpress.org/reference/functions/esc_html/`