Kritična ranjivost Drupala

Drupal, treći najpopularniji CMS, nakon WordPressa i Joomle, ranjiv je na ***SQL injection*** napad. Ranjivost je objavljena zajedno sa zakrpom 15.10.2014. No već nekoliko sati nakon toga krenuli su automatski napadi. Dakle, ako niste dogradili svoj Drupal na zakrpanu verziju 7.32, razumno je pretpostaviti da je vaš site vjerojatno provaljen.

Ranjivost je proglašena visoko kritičnom, a ironično je što je otkrivena upravo u kodu čija je zadaća da spriječi takvu vrstu napada. Napadač se može ulogirati bez autentikacije, ne ostavivši trag u logovima. Nakon toga moguće su krađe osobnih podataka, ili instalacija *backdoora*. Moguće je da su napadači, nakon postavljanja *backdoora*, instalirali zakrpu, kako bi spriječili neke druge napadače da se dočepaju sustava. Dakle, ako vam je instalirana nova verzija Drupala, a vi to niste učinili... Ne gine vam forenzička istraga. A mogli bi i razmisliti kako je vrijeme da instalirate i naučite koristiti neki *Change management software*.

Kako su ranjive sve verzije prije 7.32, kao rješenje predlaže se dogradnja na tu verziju ili instalacija zakrpe dostupne na linku https://www.drupal.org/files/issues/SA-CORE-2014-005-D7.patch [1]
Razvojni tim Drupala objavio je ranjivost [2] 15.10. na svom službenom siteu, a nakon toga, 29.10. izdano je i javno priopćenje [3] s upozorenjem na automatske napade. Korisnike se opominje da sama instalacija nove verzije neće ukloniti backdoor, ukoliko je već instaliran.

Da bi se web site što prije vratio u funkciju na siguran način, slijedite ove upute:

- Ugasite web i zamijenite ga statičnom web stranicom (radovi u tijeku).
- Upozorite administratora servera: ako se tu hostaju druge stranice i one mogu biti kompromitirane i možda imaju backdoor.
- Ako možete, nabavite novi (virtualni) server i na njemu obavite svježu instalaciju sigurne, zakrpane verzije Drupala.
- U protivnom, maknite sa servera web site i pripadajuću bazu. Kopiju sačuvajte za kasniju istragu.
- Ako redovito radite backup, vratite verziju prije 15.10. a zatim instalirajte zadnju verziju Drupala ili zakrpu. Ručno unesite sve eventualne promijenjene postavke i stranice nakon tog datuma.
- Ponovo podignite svoj web.
- Usporedite ovakav "čist" site sa spremljenom kompromitiranom verzijom, kako bi otkrili razlike, odnosno pronašli što je napadač promijenio.

pon, 2014-11-03 12:53 - Aco Dmitrović**Vijesti:** Sigurnosni propusti [4]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Source URL: https://sysportal.carnet.hr./node/1451

Links

[1] https://www.drupal.org/files/issues/SA-CORE-2014-005-D7.patch
[2] https://www.drupal.org/SA-CORE-2014-005
[3] https://www.drupal.org/PSA-2014-003
[4] https://sysportal.carnet.hr./taxonomy/term/14