Otkrivene dvije ranjivosti u programu Mozilla Firefox


Unutar programa Mozilla Firefox, drugog najkorištenijeg web preglednika na svijetu, otkrivene su dvije sigurnosne ranjivosti.

Prva ranjivost vezana je uz pop-up blocker. Firefox u pravilu ne dozvoljava web siteovima pristup lokalno spremljenim datotekama, osim ako je korisnik manualno isključio ovu opciju. Ukoliko je opcija isključena, napadač može ukrasti lokalno snimljene datoteke i osobne podatke eventualno spremljene u njima.

Mogući scenarij iskorištenja ove ranjivost je da korisnik klikne na zloćudni link kojim bi presnimio datoteku u kojoj se nalazi zloćudni kod na svoj lokalni disk. Ukoliko je u Firefoxu uključena opcija vezana uz pristup lokalnim datoteka, prije nego se zaražena datoteka učita u memoriju, iskače pop-up prozor preko kojeg korisnik odlučuje želi li pokrenuti zaraženu datoteku (koja može biti sakrivena u audio ili video formatu). Ukoliko je ova opcija isključena, zaražena datoteka se automatski pokreće, čime napadač može dobiti „read“ prava nad lokalnim datotekama.
Iako se čini da ova ranjivost pogađa samo Firefox verzije 1.x, Mozilla još nije izdala priopćenje o ranjivosti kasnijih verzija svog popularnog web preglednika.

Druga ranjivost iskorištava propust unutar phishing filtra u pregledniku. Dodavanjem određenih znakova u URL stranice, napadač može prevariti preglednik da vjeruje da je lažni site zapravo siguran. Kao i kod prošle ranjivosti, i posljednja verzija Firefoxa nije imuna na ovu vrstu napada.

Obje ranjivosti otkrio je SecuriTeam, odjel unutar tvrtke Beyond Security koja se bavi otkrivanjem i procjenama ranjivosti.

Službeno izvješće sa detaljima o ranjivosti možete pročitati ovdje:
[1]http://www.securiteam.com/securitynews/5JP051FKKE.html [2]
http://www.securiteam.com/securitynews/5MP0320KKK.html [1]

čet, 2007-02-08 13:05 - Emil Marmelić**Vijesti:** Sigurnosni propusti [3]
Kategorije: Sigurnost [4]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/61

Links
[1] http://www.securiteam.com/securitynews/5MP0320KKK.html
[2] http://www.securiteam.com/securitynews/5JP051FKKE.html
[3] https://sysportal.carnet.hr/taxonomy/term/14

[4] https://sysportal.carnet.hr/taxonomy/term/30