

Sigurnosni propust u Snortu



Prema navodima [CERT](#) [1]-a, otkriven je novi sigurnosni propust u popularnom Snortu, kojeg napadači mogu iskoristiti kako bi pokrenuli maliciozni kod na ranjivim sustavima.

Snort je besplatni alat namijenjen detekciji nedozvoljenog pristupa računalnim sustavima. Ovaj alat izvodi analizu mrežnog prometa u stvarnom vremenu, uz pripadno upozoravanje, blokiranje ili zapisivanje prometa.

Uočeni propust javlja se unutar DCE/RPC predprocesora prilikom grupiranja "SMB Write AndX" zahtjeva. Propust može rezultirati prepisivanjem spremnika uređenog po principu stoga (eng. stack) te je udaljenom napadaču omogućeno pokretanje proizvoljnog programskog koda na ranjivom računalu.

Ranjive inačice Snort paketa su:

- 2.6.1
- 2.6.1.1
- 2.6.2.1
- 2.7.0 beta 1

Na [Snort](#) [2]-ovim službenim stranicama objavljene su nove inačice za svaku od ranjivih inačica paketa. Svim korisnicima savjetuje se nadogradnja na novoobjavljene inačice.

čet, 2007-02-22 14:40 - Uredništvo **Vijesti**: [CERT](#) [3]

[Sigurnosni propusti](#) [4]

Vote: 0

No votes yet

Source URL: <https://sysportal.carnet.hr./node/91>

Links

[1] <http://www.cert.hr>

[2] <https://www.snort.org/>

[3] <https://sysportal.carnet.hr./taxonomy/term/9>

[4] <https://sysportal.carnet.hr./taxonomy/term/14>