Badlock nam puše za vratom


Ne događa se često da neki sigurnosni propust bude unaprijed oglašen, no upravo to dogodilo se sa Badlock (http://badlock.org/ [1]) napadom: propust otkriven u Samba timu čini se toliko ozbiljan da su odlučili dva tjedna unaprijed obavjestiti "Urbi et Orbi" kako će 12. travnja izdati *security advisory*, te kako očekuju napade odmah po njegovu objavljivanju.

Iako autori nisu objavili nikakve podatke o problemu, sudeći prema nazivu buga i priloženoj ikoni, moglo bi se raditi o problemu lockinga ili, danas nažalost nimalo iznenađujuće, o problemu u kriptografskom algoritmu. Situacija je u svakom slučaju toliko ozbiljna da Microsoft i Samba tim rade na istovremenom izdanju sigurnosne zakrpe.

Problem se nalazi negdje u implementaciji SMB protokola i obuhvaća i Windows računala i Samba daemon, dok autori ne spominju Appleovu implementaciju SMB protokola. Kako je SMB “kruh i pašteta” gotovo svakog IT sustava, a posebice zbog ozbiljnosti upozorenja, ovaj propust nemojte shvatiti olako već instalirajte sigurnosne zakrpe čim budu dostupne.

Administratore Linux poslužitelja posebno se upozorava na činjenicu da Samba niža od verzije 4.2 više neće biti sigurnosno održavana, što znači da za tu i starije verzije neće biti moguće (barem ne službeno) dobaviti sigurnosnu ispravku.

Stoga, budite budni i primjenite sigurnosne nadogradnje čim one budu dostupne. Upozorili bismo ovom prilikom ne samo na potrebu za nadogradnju Sambe barem na veziju 4.2, već i na to da obratite pozornost na druge uređaje koji koriste Sambu, poput NAS uređaja, za koje možda neće biti odmah dostupna nadogradnja firmware-a, što će ih ostaviti izložene napadu.

U tom slučaju valja razmotriti dvije solucije: jedna je izoliranje uređaja iz mreže do instaliranja nadogradnje firmware-a, a druga je privremena promjena konfiguracije, odnosno zamjena Samba servisa nekim drugim servisom (NFS, scp, sftp...) koji omogućuje istovjetnu ili vrlo sličnu funkcionalnost, nakon čega valja isključiti Samba daemon na uređaju te ga ponovno aktivirati (i sve vratiti na staro) tek nakon instaliranja novog firmware-a.

Ako je uređaj toliko star da ne podržava novije verzije Sambe (>=4.2), možda bi najpametnije bilo trajno zamjeniti taj protokol nekim drugim.

Savjeti su pomalo drastični, no obzirom na alarmantnost upozorenja možda bi ih bilo mudro poslušati, čak i ako se potom ispostavi da opasnost nije bila baš toliko katastrofalna.
.

pet, 2016-03-25 12:20 - Radoslav Dejanović**Vijesti:** Sigurnost [2]
Sigurnosni propusti [3]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Source URL: https://sysportal.carnet.hr/node/1630

Links
[1] http://badlock.org/
[2] https://sysportal.carnet.hr/taxonomy/term/13
[3] https://sysportal.carnet.hr/taxonomy/term/14