Let's Encrypt zablokoval nebezpečnou validaci pomocí self-signed certifikátu

Jak funguje tls-sni-01

Validační metoda `tls-sni-01` je vynálezem tvůrců projektu autority Let's Encrypt. Spočívá ve vystavení *self-signed* certifikátu na neexistující doménové jméno (například `773c7d.13445a.acme.invalid`), které obsahuje ověřovací kód. Certifikační autorita při ověřování naváže s daným doménovým jménem TLS spojení a do hlavičky SNI vloží toto speciální jméno. K úspěšnému ověření dojde, pokud server odpoví certifikátem vystaveným na dané speciální jméno.

Validační metodu `tls-sni-01` používá především oficiální klient Certbot. Je výhodná pro automatizaci, protože vyžaduje minimální konfigurační zásahy do webserveru. Není ale jediná, Let's Encrypt podporuje také validaci `http-01` spočívající ve vystavení souboru s určitým obsahem na určité cestě a `dns-01`, kde k ověření dochází umístněním TXT záznamu na doméně `_acme-challenge.<validované DNS jméno>`.

Zranitelnost sdílených hostingů

Podle zjištění Franse Roséna existují provozovatelé sdílených webhostingů, pro které ověření metodou `tls-sni-01` umožňuje získat cizí certifikát:

Kombinace těchto dvou okolností pak umožňuje získat TLS certifikát na libovolné doménové jméno hostované na stejné IP adrese. Mějme například dvojici webových prezentací, jednu na doméně `legit.example`, druhou na doméně `badguy.example`. První patří oběti, druhá útočníkovi, obě sdílí IP adresu. Útočník jednoduše požádá autoritu o certifikát na jméno `legit.example` a na výzvu autority vyrobí *self-signed* certifikát na autoritou požadované jméno, který nahraje jako certifikát pro jím ovládaný hosting `badguy.example`. Autorita se připojí na IP adresu oběti, která je shodná s IP adresou útočníka a požádá o speciální certifikát. Webserver ochotně vybere certifikát poskytnutý útočníkem, byť patří zcela jinému zákazníkovi.

Zranitelnost tedy postihuje **výlučně sdílené hostingy**, pro které jsou splněny výše uvedené podmínky. Přitom už nezáleží na žádných dalších okolnostech. Zranitelnost stejným způsobem funguje i pro inovovanou variantu ověření `tls-sni-02`, která je součástí nového standardu protokolu ACME.

Reakce Let's Encrypt

V krátké době po zjištění incidentu byla validace metodou `tls-sni-01` vypnuta. I přesto, že nejde o nejoblíbenější metodu validace (tou je `http-01`), má své uživatele a velká část z nich nemůže zcela automaticky přejít na jiný druh validace. V plánu proto je validaci opět zprovoznit v momentě, kdy bude problém nějakým způsobem vyřešen nebo obejit.

Lidé z ISRG, organizace stojící za projektem Let's Encrypt, se domnívají, že problém je možné zmírnit implementací silnějších kontrol na straně provozovatale webhostingu, tak aby si zákazník nemohl nahrát libovolný certifikát. Postižení provozovatelé jsou v kontaktu s ISRG a takové opravy by měly být brzy dostupné.

Během následujících 48 hodin chce ISRG vytvořit seznam postižených webhostingů. Jakmile bude hotový, měla by být validace `tls-sni-01` znovu zprovozněna, s tím, že pro IP adresy na seznamu bude zablokována.

Dalším krokem je pak vyvolání diskuze o budoucnosti validační metody v rámci komunity kolem Let's Encrypt a protokolu ACME. Je možné, že po zvážení všech pro a proti bude takováto validace prohlášena za zastaralou a její používání bude postupně utlumováno.