General - Transparency

Dawid Karpiński

Transparency

Wyzwanie dotyczyło bezpieczeństwa protokołu TLS (Transport Layer Security) i procesu weryfikacji certyfikatów. Celem było znalezienie subdomeny `cryptohack.org`, która używa podanego klucza publicznego RSA w swoim certyfikacie TLS.

Załączony plik do challeng'u `transparency.pem` to klucz publiczny RSA. Aby otrzymać fingerprint certyfikatu, za pomocą narzędzi `openssl rsa` oraz `openssl sha256`, przekonwertowano go do formatu DER oraz obliczono z wyniku hash SHA-256 lub SHA-1.

```
$ openssl rsa -pubin -in transparency.pem -outform der | openssl sha256
writing RSA key
SHA2-256(stdin)= 29ab37df0a4e4d252f0cf12ad854bede59038fdd9cd652cbc5c222edd26d77d2
```

W odpowiedzi na zagrożenia, Google Chrome od 2018 roku wymusza stosowanie tzw. Certificate Transparency. Każdy "Certificate Authority" (CA) musi publikować wydane certyfikaty w publicznie dostępnym logu.

Stąd, skorzystano ze strony `https://crt.sh/`, używając wyszukiwania poprzez kryterium:

```
Type: SHA-256(SubjectPublicKeyInfo)
Match: =    Search: '29ab37df0a4e4d252f0cf12ad854bede59038fdd9cd652cbc5c222edd26d77d2'
```

W wyniku otrzymano dwa certyfikaty:

crt.sh ID	Logged At	Not Before	Not After	Issuer Name
3347792120	2020-09-07	2020-09-07	2020-12-06	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
3347788342	2020-09-07	2020-09-07	2020-12-06	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Wybrano pierwszy z nich o ID 3347792120. Wśród treści certyfikatu znaleziono szukaną domenę:

```
Certificate:
    Data:
        ...
        Subject:
            commonName                = thetransparencyflagishere.cryptohack.org
```

Odwiedzenie domeny za pomocą `curl` dało ostateczną flagę.

```
$ curl -s -L thetransparencyflagishere.cryptohack.org
crypto{thx_redpwn_for_inspiration}
```