Bezpečné doručení distribučních balíčků

Karel Kočí

26.5.2018


TURRIS

Balíček?

- Meta informace (název, verze, ...)
- Soubory
- Hashe pro soubory

Indexovány a uloženy v repositářích

- Repositář obsahuje index
- Index obsahuje hashe balíčků a další meta informace

Krypto terminologie

- Hash
- Asymetrická šifra
- Kryptografický podpis
- Certifikační autorita

Útok #1: Podvrhnutí repositářů

- Vlastní server s upravenými balíčky distribuce
- Kompromitace připojení k Internetu

Ochrana #1: Podpis

- Před-distribuovaný veřejný klíč
- Podepsané balíčky nebo index repositáře (lépe index)

Útok #2: Podvrhnutí starší verze repositářů

- Kopie repositářů distribuce se známou zranitelností (Heartbleed, CVE-2016-0777 CVE-2016-0778, ...)
- Vlastní server se starší kopií repositářů distribuce
- Kompromitace připojení k Internetu

“Ochrana” #2: Porovnání verzí

Balíčky je možné pouze updatovat

- Downgrade je nutné schválit (ale jen u některých a uživatel...)
- Downgrade je občas legitimní
- Co update ze staré verze systému? (pravidelné aktualizace)
- Co instalace?

Ochrana #2: HTTPS a SSL

- Server s repositáři se ověřuje validním certifikátem
- Identita serveru (jeho DNS jméno a pod.) je podepsána

Útok #3: Vlastní certifikát

- Kopie repositářů distribuce se známou zranitelností
- Vlastní server se starší kopií repositářů distribuce
- Vlastní certifikát s totožnou identitou od "důvěryhodné"autority

Ochrana #3: Certification pinning

- Omezit počet důvěryhodných certifikátů (pár vybraných)
- Vždy mějte vlastní certifikační autoritu jako fallback!
- Tak trochu hra v kostky

Útok #4: Podvrhnutí DNS

- Kopie repositářů distribuce se známou zranitelností
- Vlastní server se starší kopií repositářů distribuce
- Kompromitace používaného DNS serveru (např: otrávení) a podvrhnutí vlastní IP

Ochrana #4: DNSSEC

- Kontrola správnosti DNS odpovědi pomocí podpisů
- Odpověď je stejná tak jak ji poskytuje příslušný autoritativní server

- Nutné správné nastavení systému nejenom aplikace
- Nízké uvědomění uživatelů o užitečnosti DNSSEC

Útok #5: BGP leak IP

- Kopie repositářů distribuce se známou zranitelností
- Vlastní server se starší kopií repositářů distribuce
- Zneužití BGP ohlašování a přesměrování
- Vlastní důvěryhodný certifikát s totožnou identitou (Let 's Encrypt)

Ochrana #5: RPKI

- Kryptografické ověření přidělení ohlašované IP adresy

- Nižší rozšířenost
- Uživatelsky nekontrolovatelné a nevynutitelné
- Výrazně složitý útok

Děkuji za pozornost

Udržujte svoje systémy aktuální!

Nastavte si DNSSEC!