Distribuce malware přes doménu polyfill.io

> Aktuálně (27. 6.) byla doména suspendována doménovým registrátorem, přestala fungovat a malware tak již není pomocí této domény distribuován. Přesto stále doporčujeme odstranit načítání skriptů z níže uvedených domén.

Upozorňujeme na situaci, kdy legitimní doména polyfill[.]io, která byla použita pro distribuci javascriptové knihovny polyfill.js, byla odkoupena čínským akterém a nyní je používána pro distribuci malware.

Doporčujeme si tedy zkontrolovat vaše webové stránky a webové aplikace, zda nenačítají JavaScriptové a CSS knihovny z domén `cdn.polyfill.io`, `bootcss.com`, `bootcdn.net` nebo `staticfile.org`. Pokud ano, doporučujeme načítání těchto skriptů odstranit – v dnešní době moderních prohlížečů již nejsou potřeba.

Dále doporučujeme obecně nenačítat Javascriptové knihovny a CSS z externích zdrojů (domén). Kromě rizika distribuce malware, jako se děje v tomto případě, zda také existuje riziko nedostupnosti externích zdrojů. V případě využití externích zdrojů doporučujeme využívat technologii Subresource Integrity (SRI).

Pro bezpečný vývoj webových aplikací je možné aplikovat relevantní doporučení z Bezpečnostních doporučení pro vývoj otevřeného softwaru ve veřejné správě, které vydal NÚKIB ve spolupráci s MV v roce 2022.

Další informace

- https://sansec.io/research/polyfill-supply-chain-attack
- https://thehackernews.com/2024/06/over-110000-websites-affected-by.html

- https://www.theregister.com/2024/06/25/polyfillio_china_crisis/
- https://zdrojak.cz/clanky/sluzba-polyfill-io-byla-napadena-hackery/ - český článek ne serveru Zdroják.cz

Klasifikace

TLP:CLEAR

Autor

Národní úřad pro kybernetickou a informační bezpečnost

Datum

27. 06. 2024

Obsah

Reakce

Zatím žádné reakce na článek