مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

POLYFILL Supply Chain Attack on Websites

Tracking #:432316031

Date:08-07-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a widespread supply chain attack involving the polyfill[.]io domain.

TECHNICAL DETAILS:

A widespread supply chain attack involving the polyfill.io domain is observed and this domain, previously used to provide compatibility libraries for older browsers, was compromised and redirected users to malicious websites. While the domain itself is suspended, millions of websites still reference it, potentially impacting user security. A Chinese company called Funnull acquired the domain and GitHub account in February 2024 and Funnull modified Polyfill.js to inject malicious code into websites that included scripts from cdn.polyfill[.]io.

Details:

- **Impact:** Over 380,000 websites were potentially affected, including major platforms were identified using the malicious script. It redirects to scam sites, Theft of sensitive user, Unauthorized code execution on user devices data.
- **Potential Future Threats:** Identified another potentially malicious domain, that have been used by the same actor to spread malware since at least June 2023: bootcdn[.]net, bootcss[.]com, staticfile[.]net, staticfile[.]org, unionadjs[.]com, xhsbpza[.]com, union.macoms[.]la, newcrbpc[.]com. exhibiting similar redirection behaviour. Websites referencing this domain should also be investigated.

RECOMMENDATIONS:

- Website Owners: Immediately review website code and remove all references to "polyfill.io" and its associated domains (".com", "cdn.polyfill.io").
- Block the Malicious Domains.
- Consider alternative secure polyfill providers.
- IT Security Teams: Scan web infrastructure for references to polyfill[.]io and implement website monitoring solutions to detect suspicious redirects.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://sansec.io/research/polyfill-supply-chain-attack