Mphasis SOC – Information Security News
Date & Time Issued: 4-JULY-2024, 2:00 IST

Title	**Polyfill Fuels Supply Chain Concerns with Malicious Redirects**
Summary	• The recent large scale supply chain attack conducted via multiple CDNs, namely Polyfill.io, BootCDN, Bootcss, and Staticfile that affected anywhere from 100,000 to tens of millions of websites has been traced to a common operator, according to researchers. • Researchers discovered a public GitHub repository where the purported operators of Polyfill.io had accidentally exposed their Cloudflare secret keys. • By using these leaked API keys, which were still active, researchers were able to establish that a common operator was behind all four domains, and the wider supply chain attack.
Severity	Medium
Attack Vectors	• Security researchers and open source intel (OSINT) enthusiasts discovered a GitHub repository associated with the polyfill.io domain involved in a large-scale supply chain attack that is now believed to have impacted tens of millions of websites. • The secrets leaked in the repository enabled researchers to attribute the supply chain attack involving all 4 CDN services, namely, Polyfill.io, BootCDN, Bootcss, and Staticfile, to a single entity. The discovery was made due to the collaborative effort between researcher Ze-Zheng Wu, a pseudonymous user mdmck10, and the security research group, MalwareHunterTeam. • Ze-Zheng Wu, a developer and a PhD candidate based in Hangzhou, China, discovered a GitHub repository titled, "data.polyfill.com" that appeared to contain the backend source code associated with the website. Dot env (.env) files are used by developers and sysadmins to store secrets such as API keys and tokens, environment variables, and configuration settings. As such, these files should be secured with restrictive permissions and be heavily guarded from the public. • The exposed file, as also seen by BleepingComputer, contains a Cloudflare API token, Cloudflare Zone ID (of the Polyfill.io domain), and Algolia API keys, among other values.

Indicator of Compromise	INDICATOR TYPE	INDICATORS
	URLs	• https[:]//kuurza.com/redirect?from=bitget • https[:]//www.googie-anaiytics.com/html/checkcachehw.js • https[:]//www.googie-anaiytics.com/ga.js • https[:]//cdn.bootcss.com/highlight.js/9.7.0/highlight.min.js • https[:]//union.macoms.la/jquery.min-4.0.2.js • https[:]//newcrbpc.com/redirect?from=bscbc
	Domains	• bootcdn[.]net • staticfile[.]net • staticfile[.]org • unionadjs[.]com • xhsbpza[.]com

Recommendations	• Immediately replace any usage of Polyfill.io, BootCDN, Bootcss, and Staticfile with safe alternatives provided by trusted CDN providers like Cloudflare and Fastly. • Conduct thorough audits of your web environment and look for any unusual or unauthorized modifications. • Incident response handlers should search their SIEM logs for connections to the compromised CDN domains. • Ensure restrictive permissions on sensitive files like .env files and avoid exposing such files in public repositories. • Stay updated on the latest developments and additional domains that might be used by the attackers. • Employ tools like Polykill.io from Leak Signal to identify and replace websites using the compromised services. **NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre -Prod or test environment before implementing. diligence and impact analysis.**

References	• https://sansec.io/research/polyfill-supply-chain-attack • https://www.bleepingcomputer.com/news/security/polyfillio-bootcdn-bootcss-staticfile-attack-traced-to-1-operator/

The information contained in this message is proprietary. It is for Mphasis and its customers only.
Copyright © 2024. All rights reserved by Mphasis.