jscrambler

Web supply chain attacks

Mitigation overview

A data sheet by Jscrambler

Key business threats

Loss of customer data including payment card info, user credentials, or personally identifiable information (PII).

Loss of sales and customer trust, as customers will be wary after the attack takes place.

Heavy GDPR/CCPA fines which can amount to several million dollars.

Potential class-action lawsuits, as affected customers can take legal action in the aftermath of the attack.

How do web supply chain attacks work?

Finding the weakest link in the supply chain
Instead of breaching a large enterprise's server, attackers go after the third-party code that this company uses. And the providers of this third-party code often have fewer resources allocated to security, making them easier targets.

Inserting malicious code into a third-party
After breaching the third-party provider, attackers insert the malicious code into the legitimate script that is sourced to all the different websites that use it.

Reaching the desired targets downstream
Because the path to the script file stays the same, network defenses fail to identify the malicious code. It immediately starts being served by all websites that use it.

Breaching thousands of companies in one go
The malicious code is then capable of executing in every user session for all affected websites. It usually skims credit cards (Magecart) or leaks user data to attackers' drop servers.

The web is full of weak links

Your third-party code suppliers don't have enterprise-grade security. You must protect your client-side against web supply chain attacks.

70%
Average web application code coming from third-party providers.

82%
Websites running third-party scripts with vulnerabilities.

2 million+
Websites breached by Magecart web skimmers.

Business losses are huge

After the initial period of negative PR and customer distrust, **companies face significant GDPR/CCPA fines and class-action lawsuits.**

$26M
British Airways fine following the 2018 Magecart web supply chain attack.

$650M
Class action lawsuit against British Airways (Magecart).

$6.5M
Class action lawsuit against Ticketmaster (Magecart).

Low-effort, high gain attacks

Attackers are highly motivated to pursue web supply chain attacks, as they **breach a single, ill-secured company (or developer) and attack thousands of companies at once.**

The second
quarter of 2023 saw 855 accounts breached every minute.

88000
Malicious open source packages had been discovered in 2022

60%
of organizations work with over 1 000 third parties.

Common Approaches

Network Defenses (WAF)

Approach
Block unknown or untrusted connections to the server.

Advantages
Prevent potentially dangerous connections and server attacks like SQL injection.

Limitations
Doesn't detect what happens at the client side; can't mitigate web supply chain attacks.

Content Security Policy (CSP)

Approach	Advantages	Limitations
Filter connection to external sources based on a whitelist.	Some level of control of third-party scripts (completely allow or disallow them).	Plenty of bypasses. Doesn't effectively prevent data leakage. Lacks granularity.

Subresource Integrity (SRI)

Approach	Advantages	Limitations
Only load scripts that pass an integrity check.	Prevent loading a script if its content changes.	Blocks legitimate updates. Not all providers use SRI.

Domain Sinkholing

Approach	Advantages	Limitations
Redirects the flow of requests to other servers.	Prevent the connection to attackers' drop servers.	Bypassable by changing the attack injection.

Sandboxing

Approach	Advantages	Limitations
Isolates third-party code inside individual iFrames.	Filters events based on a static whitelist.	Introduces performance drops and new race conditions that can break the app.

Mitigation With Webpage Monitoring

Key business threats

Protect sensitive user data by detecting and blocking client-side data exfiltration attacks like Magecart in real-time.

Gain complete visibility and control of the behavior of every third-party script running on your website.

Jscrambler detects and controls malicious client-side behavior in real-time

Webpage Inventory
Complete visibility of every script and network request that have been loaded or changed something on your website. This enables a straightforward vetting of resources, making it easy to identify malicious client-side behavior.

Third Party Management
Simple onboarding and vetting of third-party scripts, with full observability of each script and a powerful rules engine that allows controlling their behaviors.

Improve compliance with regulations such as PSD2, GDPR, CCPA, HIPAA, PCI DSS, and standards like ISO 27001 and NIST.

Safeguard revenue streams, by ensuring that no client-side attacks are diverting your users, tricking them, and damaging your reputation and conversion rate.

User Data Management
Dashboard with details of how user data is being handled at the client-side and data leakage insights. When coupled with Jscrambler's rules engine, it allows controlling where sensitive data can and cannot be sent to, preventing data exfiltration.

Webpage Threat Mitigation
Powerful and granular rules engine that provides full control of each script running on your website. This allows blocking any script in real-time if it exhibits malicious or disallowed behavior (e.g. accessing a payment form, sending sensitive data to an unknown domain, tampering with native rowser functions).

If you want to know more about how Jscrambler can help you prevent client-side attacks, don't hesitate to contact us.

hello@jscrambler.com | +1 650 999 0010