Suspected Optimizely supply chain attack puts malicious JavaScript on major websites



A suspected supply chain attack on Optimizely led to malicious JavaScript loading on popular sites, including Zoom, CNN, BBC, Salesforce and GitLab. The scripts target crypto and payment data and iOS vulnerabilities.

- The incident is described as a suspected supply chain attack involving Optimizely.
- Malicious JavaScript was loaded on numerous popular websites.
- Sites named include Zoom, CNN, Fox News, BBC, Salesforce and GitLab.
- The scripts aim to steal cryptocurrency and payment information.
- They also attempt to exploit vulnerabilities in iOS devices.

What was reported

BleepingComputer reports a suspected supply chain attack involving Optimizely. As a result, malicious JavaScript was loaded on numerous well-known websites, among them Zoom, CNN, Fox News, BBC, Salesforce and GitLab.

What the scripts do

According to the report, visitors were exposed to scripts built to steal cryptocurrency and payment information and to exploit vulnerabilities in iOS devices. The source excerpt does not give further technical detail, so the scope, timeline and remediation status should be confirmed from the vendor and the original report.

Why it matters

The case shows how a third-party script supplier can become a delivery path into otherwise trusted websites. Institutions that load external JavaScript on customer-facing pages, particularly payment or login pages, inherit the risk of that supplier even if their own systems are untouched.

The attack is described as suspected, so details may change as the investigation continues. A calm, evidence-based review of your own third-party script exposure is the sensible response.

What to do now

1. Inventory all third-party scripts, including Optimizely, loaded on your public websites and apps.
2. Check whether Optimizely is used by your web properties or by vendors acting for you.
3. Review web logs and monitoring for unexpected script changes or unfamiliar external domains.
4. Apply a Content Security Policy and integrity controls to limit what external scripts can run, especially on payment and login pages.
5. Ask affected vendors for incident status and be ready to notify customers and regulators if your users were exposed.