Suspected Optimizely supply chain attack loads malicious JavaScript on major brand websites



A suspected supply chain attack on Optimizely caused malicious JavaScript to load on many popular websites. The scripts aim to steal cryptocurrency and payment data and to exploit iOS vulnerabilities.

- The incident is described as a suspected supply chain attack targeting Optimizely.
- Malicious JavaScript was loaded on numerous popular websites.
- Sites named in the report include Zoom, CNN, Fox News, BBC, Salesforce and GitLab.
- The scripts are designed 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 served on a number of well-known websites, among them Zoom, CNN, Fox News, BBC, Salesforce and GitLab.

The report describes the scripts as built to steal cryptocurrency and payment information, and to exploit vulnerabilities in iOS devices. The excerpt available to us does not give further detail on the mechanism, the timeline or the scale of exposure, so those points should be confirmed against the full report and any vendor statement.

Why it matters

This kind of incident shows how a third-party script or service can put malicious code in front of visitors even when the website owner's own systems have not been breached. Institutions that embed external JavaScript on customer-facing pages, particularly payment or login pages, share this exposure.

Recommended approach

There is no need for alarm, but a short review is justified. Establish whether Optimizely or similar third-party scripts are used in your web properties, watch for official guidance from the vendor, and check that you can detect unexpected changes in the scripts your pages load.

What to do now

1. Inventory all third-party and externally hosted scripts on public websites and apps, and confirm whether Optimizely is among them.
2. Follow Optimizely's and affected organisations' official advisories and apply any recommended steps.
3. Review recent web logs and security monitoring for unexpected script sources or changed script content on payment and login pages.
4. Apply integrity controls such as Content Security Policy and Subresource Integrity where feasible, and limit third-party code on sensitive pages.
5. If exposure is confirmed, assess whether customer payment data is affected and follow your incident response and regulatory notification procedures.