Optimizely Web Experimentation Supply Chain Attack – Malicious JavaScript Injection

Severity Level: CRITICAL

Components Affected

- Optimizely Web Experimentation customer projects and Project JavaScript
- Websites and online portals loading affected Optimizely JavaScript snippets
- Payment, checkout and cryptocurrency-related pages using affected snippets
- Visitors' web browsers executing injected third-party JavaScript
- iPhone and iPad devices exposed to attempted mobile exploit delivery

Overview

On 16 November 2026, an attacker exploited a vulnerability in the account-signup flow of Optimizely Web Experimentation to impersonate customer users and insert malicious JavaScript into customer projects. Security researchers at Report URI identified 188 affected JavaScript snippets associated with 178 organizations among 1,611 snippets examined. The incident involved a trusted third-party script dependency and did not necessarily mean that the affected organizations' own servers or networks were breached.

Optimizely reports that the first malicious project modification occurred at 07:51 UTC on 16 November 2026. The vulnerability was fixed at 16:10 UTC and the injected code removed from affected projects by 22:24 UTC. The vendor's forensic investigation continues. No confirmed compromise of a Sri Lankan government institution has been established in the reviewed public reporting.

Description

The attack abused a weakness in Optimizely's signup workflow to gain unauthorized administrator-level access to selected Web Experimentation projects. The attacker modified Project JavaScript, which is distributed to visitors as part of an otherwise legitimate website snippet. This allowed malicious code to execute in visitors' browsers when affected pages were opened.

- **Attack Vector –** The attacker impersonated customer users without obtaining their passwords and changed project-level JavaScript. This was not reported as a customer-password breach.
- **Malware Delivery –** Affected snippets could load a second-stage payload from 1688360[.]cc/track.js; vendor-reported infrastructure includes pay.pay-cloud[.]online and pay-relay.wordpressadmin001.workers[.]dev.
- **Malicious Capabilities –** Researchers observed payment-card skimming, cryptocurrency address replacement and conditional collection of browser-readable cookies and page screenshots.
- **Mobile Exploitation –** The campaign also attempted to route iPhone and iPad visitors to iOS exploit content. Delivery attempts do not establish a successful device compromise.

Impact

- Potential theft of card numbers, expiry dates and CVV details entered into payment forms on affected pages.
- Unauthorized redirection of cryptocurrency transactions through replacement of wallet addresses.
- Conditional exposure of browser-readable cookies, page URLs and screenshots in malicious requests.
- Attempted exploitation of vulnerable iPhone and iPad devices visiting affected websites.
- Financial fraud, sensitive information exposure and loss of public trust in affected online services.

Solution/ Workarounds

Immediate investigation and response:

- Identify websites and government portals that used Optimizely Web Experimentation during 16 November 2026; obtain an affected-project confirmation and site-specific exposure window from Optimizely.
- Review Project JavaScript, changes to experiment code, administrators and available change records. Preserve historical script samples and relevant evidence.
- Search DNS, proxy, WAF, CSP and endpoint telemetry for 1688360[.]cc, pay-cloud[.]online, pay-relay.wordpressadmin001.workers[.]dev and related suspicious requests.
- Investigate payment-card and cryptocurrency transactions made on confirmed affected pages during the relevant exposure period; coordinate with fraud and privacy teams where required.
- Investigate mobile devices where credible indicators indicate exploit content was accessed, and update supported iOS/iPadOS devices promptly.

Recommended preventive and monitoring measures:

- Implement a restrictive Content Security Policy (CSP) for script and outbound connections, and monitor CSP violation reports.
- Limit third-party JavaScript on login, payment and sensitive-data pages; monitor script and configuration changes.
- Restrict Optimizely administrative privileges and enforce strong access controls. Do not perform blanket password or API-token resets solely due to this incident.
- Block validated attacker-controlled destinations where appropriate. Do not block the legitimate cdn.optimizely.com domain solely because it distributes Optimizely snippets.

Organizations are strongly advised to review affected web integrations, preserve evidence and report suspected or confirmed compromise to Sri Lanka CERT through the official incident reporting channels.

Reference

- Optimizely – Security Incident Initial Report (17 November 2026)
- Report URI – Technical Analysis (16 November 2026)
- Netskope Threat Labs – Optimizely Snippet Compromise (17 November 2026)

Disclaimer

The information provided herein is on an "as is" basis, without warranty of any kind.