Optimizely Web Experimentation scripts hijacked on at least 178 organisations' sites



Optimizely says an attacker exploited a flaw to plant malicious code in scripts served to customer websites. Report URI says visitors to at least 178 organisations, including CNN, the BBC and Zoom, received it.

- An attacker exploited a flaw in Optimizely Web Experimentation, according to Optimizely.
- Malicious code was planted in some scripts that customer sites load from the service.
- Report URI, which monitors website scripts, says visitors to at least 178 organisations received the code.
- Named affected sites include CNN, the BBC and Zoom.
- The headline refers to a card skimmer and iOS exploit kits; the excerpt available does not describe the code's behaviour in detail.

Optimizely said that an attacker exploited a flaw in its Web Experimentation product and used it to insert malicious code into some of the scripts that customers' websites load from the service. The company disclosed the incident early today.

Report URI, a firm that monitors the scripts websites run, says visitors to sites operated by at least 178 organisations received the code yesterday. The organisations it names include CNN, the BBC and Zoom.

What is known

The source headline says the affected scripts delivered a card skimmer and iOS exploit kits. The text available to us is partial, so we do not have details on how the code behaved, which flaw was involved, or what remediation Optimizely has issued. Readers should wait for the vendor's own advisory before drawing conclusions.

Why it matters

The incident shows the risk of third-party scripts: code served from a vendor's platform runs with the trust of the website that embeds it, so a compromise at the vendor reaches every customer's visitors at once. Organisations that process card payments or serve mobile users should treat such scripts as part of their own attack surface.

Suggested next steps

Institutions should first establish whether they use Optimizely Web Experimentation on any public site or app, then follow the vendor's guidance and review what their pages loaded during the reported window.

What to do now

1. Check whether any public website, portal or app uses Optimizely Web Experimentation.
2. Follow Optimizely's advisory and apply any remediation it publishes.
3. Review web server, tag manager and content security logs for script changes during the reported window.
4. If payment pages were affected, inform your acquirer and assess exposure of card data under PCI DSS.
5. Maintain an inventory of third-party scripts and consider integrity controls such as a restrictive content security policy.