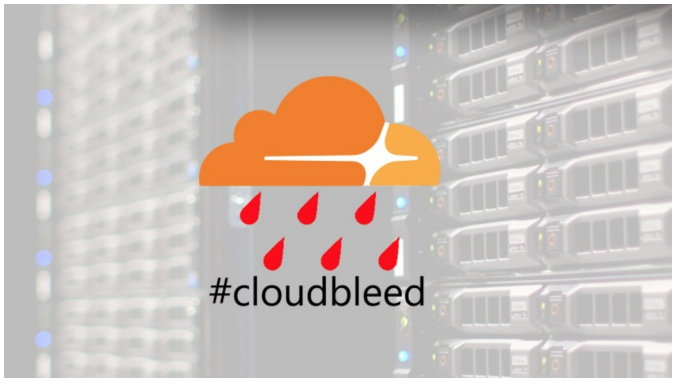
Cloudflare reveals the extend of "Cloudbleed," the bug leading to the mass leaking of encrypted browsing sessions-- it was triggered over 1 million times in the past 6 months before it was patched.



According to the post-mortem by Cloudflare CEO Matthew Prince there is "no evidence" the bug was maliciously exploited, even if it had the "potential to be much worse." In total the bug was triggered 1.2 million times from 6500 websites, and the company is still going through Google, Microsoft Bing and Yahoo search engine caches to scrub leaked data off the memory of cached sites.

“We’ve successfully removed more than 80000 unique cached pages," Prince writes. "That underestimates the total number because we’ve requested search engines purge and recrawl entire sites in some instances."

The Cloudbleed bug was discovered last month by Google Project Zero researcher Tavis Ormandy, and the vulnerable code was first introduced in the Cloudflare HTML parser back in 22 September 2016. The company says leaks included internal Cloudflare headers and customer cookies, but it insists no passwords, encryption keys, paymend card data or health records were leaked.

According to Prince, the bug was triggered only when a webpage moving through the Cloudflare network carried HTML ending with an un-terminated attribute while a number of Cloudflare features were turned on. This lead to edge servers allowing data to run over the buffer, and return non-encrypted memory. Initially the bug affected a small number of sites, but 13 February parser update brought new triggers to the bug and expanded the number of impacted sites from 180 to 6457.

The vulnerability was patched out on 18 February after Ormandy privately disclosed it to the company.

“The nightmare scenario we have been worried about is if a hacker had been aware of the bug and had been quietly mining data before we were notified by Google’s Project Zero team and were able to patch it,” Prince says. “For the last 12 days we’ve been reviewing our logs to see if there’s any evidence to indicate that a hacker was exploiting the bug before it was patched. We’ve found nothing so far to indicate that was the case.”

Cloudflare customers who find any leaked cached data should send a link to the caches to the company.

Go Quantifying the Impact of "Cloudbleed"