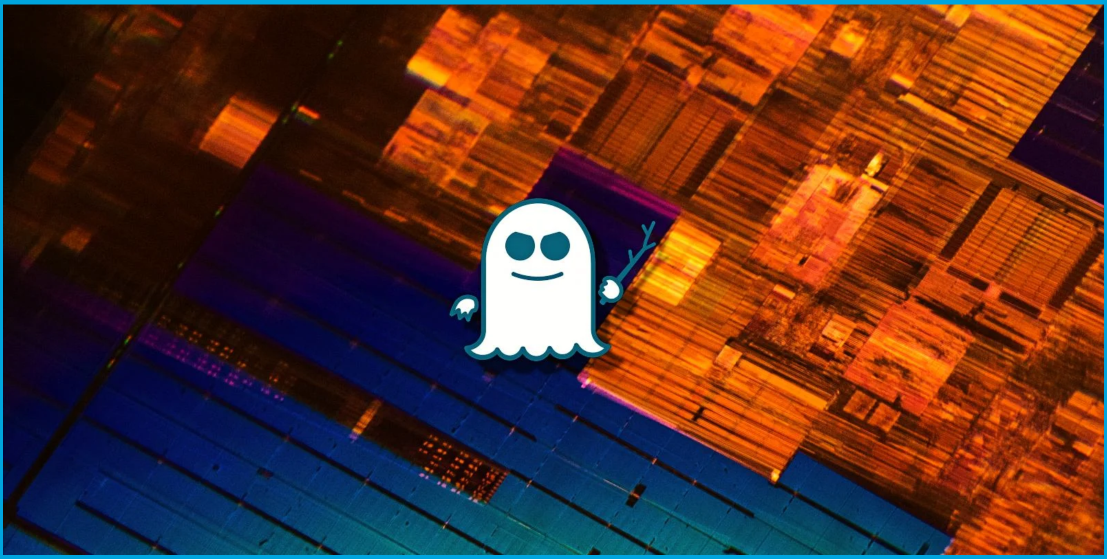
Security Newsletter

22 March 2021

Subscribe to this newsletter

Google: This Spectre proof-of-concept shows how dangerous these attacks can be



Google has released a proof of concept (PoC) code to demonstrate the practicality of Spectre side-channel attacks against a browser's JavaScript engine to leak information from its memory.

"The web platform relies on the origin as a fundamental security boundary, and browsers do a pretty good job at preventing explicit leakage of data from one origin to another," explained Google's Mike West.

"Attacks like Spectre, however, show that we still have work to do to mitigate implicit data leakage. The side-channels exploited through these attacks prove that attackers can read any data which enters a process hosting that attackers' code. These attacks are quite practical today, and pose a real risk to users."

Read More on ZDNet

Even More on Google Security Blog

More #News

- Hacking group used 11 zero-days to attack Windows, iOS, Android users
- Apple May Start Delivering Security Patches Separately From Other OS Updates
- Facebook expands support for security keys to iOS and Android
- Tax-Themed Phishing Campaign Emerges
- Australian law enforcement used encryption laws 11 times last year
- Swiss hacker charged for leaking proprietary source code
- Google Cloud: Here are the six 'best' vulnerabilities security researchers found last year
- Twitter now supports multiple 2FA security keys on mobile and web

#Breach Log

- Acer hit by $50 million ransomware attack
- XcodeSpy malware targets iOS devs in supply-chain attack
- Mimecast: SolarWinds hackers stole some of our source code
- WeLeakInfo Leaked Customer Payment Info
- FBI: Over $4.2 billion officially lost to cybercrime in 2020

#Patch Time!

- GitLab Critical Security Release
- Microsoft Defender adds automatic Exchange ProxyLogon mitigation
- Critical F5 BIG-IP vulnerability now targeted in ongoing attacks
- Critical RCE Flaw Reported in MyBB Forum Software
- Flaws in Two Popular WordPress Plugins Affect Over 7 Million Websites

#Tech and #Tools

- A free and open WIDS system to defend your wireless networks.
- Microsoft's Azure SDK site tricked into listing fake package
- The Linux kernel bugs that surfaced after 15 years
- Attack Surface Analysis - Custom Protocol Handlers
- https://securitylab.github.com/research/one_day_short_of_a_fullchain_sbx
- GitHub: How we found and fixed a rare race condition in our session handling
- Framework for tracking personal Bluetooth devices via Apple's massive Find My network

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with a diverse team of 1,600 people serving over 26 million customers across Europe, Australia and the US. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and is an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us