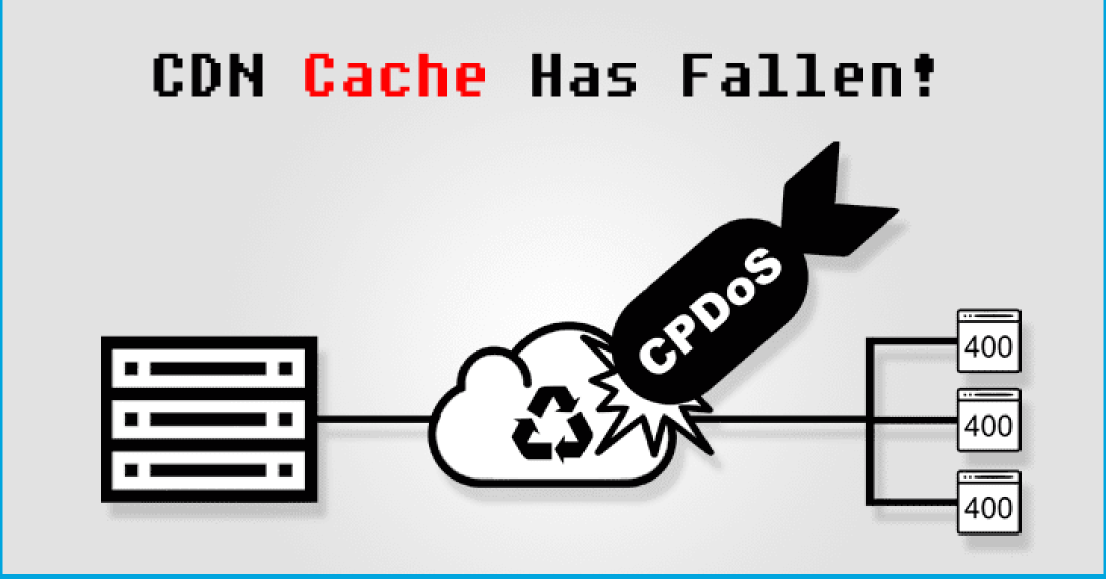
kindred

Security Newsletter

28 October 2019

Subscribe to this newsletter

New Cache Poisoning Attack Lets Attackers Target CDN Protected Sites



A team of German cybersecurity researchers has discovered a new cache poisoning attack against web caching systems that could be used by an attacker to force a targeted website into delivering error pages to most of its visitors instead of legitimate content or resources. The issue could affect sites running behind reverse proxy cache systems like Varnish and some widely-used Content Distribution Networks (CDNs) services, including Amazon CloudFront, Cloudflare, Fastly, Akamai, and CDN77. In brief, a Content Distribution Network (CDN) is a geographically distributed group of servers that sit between the origin server of a website and its visitors to optimize the performance of the website.

Dubbed CPDoS, short for Cache Poisoned Denial of Service, the attack resides in the way intermediate CDN servers are incorrectly configured to cache web resources or pages with error responses returned by the origin server. "The problem arises when an attacker can generate an HTTP request for a cacheable resource where the request contains inaccurate fields that are ignored by the caching system but raise an error while processed by the origin server."

With CPDoS, a malicious client can block any web resource that is distributed via Content Distribution Networks (CDNs) or hosted on proxy caches. Note, that a single crafted request is sufficient to restrain all subsequent requests from accessing the targeted content.

Read More TheHackerNews

Even More

Swedish police cleared to deploy spyware against crime suspects

Sweden's police force has been granted new powers this week, including the ability to deploy spyware on suspects' devices to intercept encrypted communications and turn on microphones and cameras. The new technical capabilities granted to Swedish police are part of a 34-point plan to upgrade law enforcement powers when investigating gang or violent crimes.

Damberg said that granting police the legal and technical capabilities to intercept encrypted communications was a top priority, as they were being left behind by criminal groups who now often use services like Signal and WhatsApp to coordinate operations. The minister told local press [1, 2, 3, 4] that 90% of all the communications police have intercepted for investigations in recent years have been encrypted.

But unlike countries like Australia, where the local government has passed a law forcing tech companies to introduce encryption backdoors, Swedish police will take the sensible route -- aka the German route. More than a decade ago, German authorities began deploying a malware strain named the Bundestrojaner (Federal Trojan) as part of their investigations. How Swedish authorities will do this is unclear, but there are at least two routes. They can create the malware themselves, or they can buy it from contractors. The last option has been popular with law enforcement agencies across the world, and there's now a booming market for companies that sell hacking tools and exploits (also referred to as lawful intercept tools) to law enforcement agencies. The new rules and capabilities are set to enter into effect on March 1, 2020. According to Damberg, police can only use these new capabilities if the crime someone is suspected is punishable by a penalty of four years or higher.

Read More on ZDNet

More #News

- Traditional perimeter-based network defense is obsolete—transform to a Zero Trust model
- Hacker Plants Keylogger Devices on Company Systems Faces 12yr in Jail
- FBI issues warning about e-skimming (Magecart) attacks
- Cachet Financial Reeling from MyPayrollHR Fraud
- Vietnamese student behind Android adware strain that infected millions
- FTC Issues Guidance On Protecting Against SIM Swap Attacks
- PSD2 Authentication Deadline Extended: Here's What's Next
- Alexa and Google Home phishing apps demonstrated by researchers
- Scammers Behind €10 Million BEC Fraud Arrested in Spain
- Stealthy Microsoft SQL Server Backdoor Malware Spotted in the Wild
- Ransomware Attack Shuts Down City of Johannesburg's Systems
- Major German manufacturer still down a week after getting hit by ransomware
- Hacker Breached Servers Belonging to Multiple VPN Providers
- Office 365 Now Warns About Suspicious Emails with Unverified Senders
- Zappos' Offer to Breach Victims: A 10 Percent Discount
- Don't look now, but Pixel 4's Face Unlock works with eyes closed
- Avast, NordVPN Breaches Tied to Phantom User Accounts

#Patch Time!

- Chrome 78 Released With DoH, 37 Security Patches

#Tech and #Tools

- Public keys are not enough for SSH security
- PowerForensics: provides an all in one platform for live disk forensic analysis
- Responsible denial of service with web cache poisoning
- Introducing Jib — build Java Docker images better
- Falco: Container Native Runtime Security
- Don't open that XML: XXE to RCE in XML plugins for VS Code, Eclipse, Theia, …
- Bypassing Authentication on SSH Bastion Hosts
- Stealthily Backdooring CMS Through Redis' Memory Space
- Utilizing Reverse Proxies to Inject Malicious Code & Extract Sensitive Information
- Active Directory administrative tier model

Kingred Group is growing, so does the Group Security team! We're looking for new talented professionals to come join us. You can find all our open vacancies on our career page.

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