kindred

Security Newsletter

25 May 2020

Subscribe to this newsletter

New DNS Vulnerability Lets Attackers Launch Large-Scale DDoS Attacks

Israeli cybersecurity researchers have disclosed details about a new flaw impacting DNS protocol that can be exploited to launch amplified, large-scale distributed denial-of-service (DDoS) attacks to takedown targeted websites. Called NXNSAttack, the flaw hinges on the DNS delegation mechanism to force DNS resolvers to generate more DNS queries to authoritative servers of attacker's choice, potentially causing a botnet-scale disruption to online services.

Following responsible disclosure of NXNSAttack, several of the companies in charge of the internet infrastructure, including PowerDNS (CVE-2020-10995), CZ.NIC (CVE-2020-12667), Cloudflare, Google, Amazon, Microsoft, Oracle-owned Dyn, Verisign, and IBM Quad9, have patched their software to address the problem. The DNS infrastructure has been previously at the receiving end of a rash of DDoS attacks through the infamous Mirai botnet, including those against Dyn DNS service in 2016, crippling some of the world's biggest sites, including Twitter, Netflix, Amazon, and Spotify.

The researchers said the attack can amplify the number of packets exchanged by the recursive resolver by as much as a factor of more than 1,620, thereby overwhelming not only the DNS resolvers with more requests they can handle, but also flood the target domain with superfluous requests and take it down. What's more, using a botnet such as the Mirai as a DNS client can further augment the scale of the attack. It's highly recommended that network administrators who run their own DNS servers update their DNS resolver software to the latest version.

Read More on TheHackerNews

More #News

- New Tool Can Jailbreak Any iPhone and iPad Using An Unpatched 0-Day Bug
- Hackers leak credit card info from Costa Rica's state bank
- Discord client turned into a password stealer by updated malware
- Chrome 83 arrives with enhanced security and privacy controls
- Phishing Attack Bypassed Office 365 MFA through custom app permissions
- Signal to move away from using phone numbers as user IDs
- Home Chef announces data breach after hacker sells 8M user records
- Ukraine Nabs Suspect in 773M Password 'Megabreach'
- New Spectra attack breaks the separation between Wi-Fi and Bluetooth

#Patch Time!

- Adobe "out of band" critical patch – get your update now!
- New Bluetooth Vulnerability Exposes Billions of Devices to Hackers

#Tech and #Tools

- API Management and DevOps
- terragoat: Vulnerable by design Terraform environment (education purpose)
- Virtual AppSec Days Summer of Security 2020
- shotlooter: finds sensitive data inside the screenshots uploaded to prnt.sc
- Ligolo : Reverse Tunneling made easy for pentesters, by pentesters
- Pentesting 101: Working With Exploits
- Kubetap Documentation
- Introducing Shuffle — an Open Source SOAR platform part 1
- Google fuzzing dictionaries
- Update on JavaScript Skimmer Enhancements
- Oriana: threat hunting tool leveraging Windows events to build relationships
- Red Team Attack Operation RT-011 - Phishing - Fake Laptop Upgrade
- Running dodgy programs safely with Windows Sandbox

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

If you no longer wish to receive this newsletter, you can unsubscribe from this list.