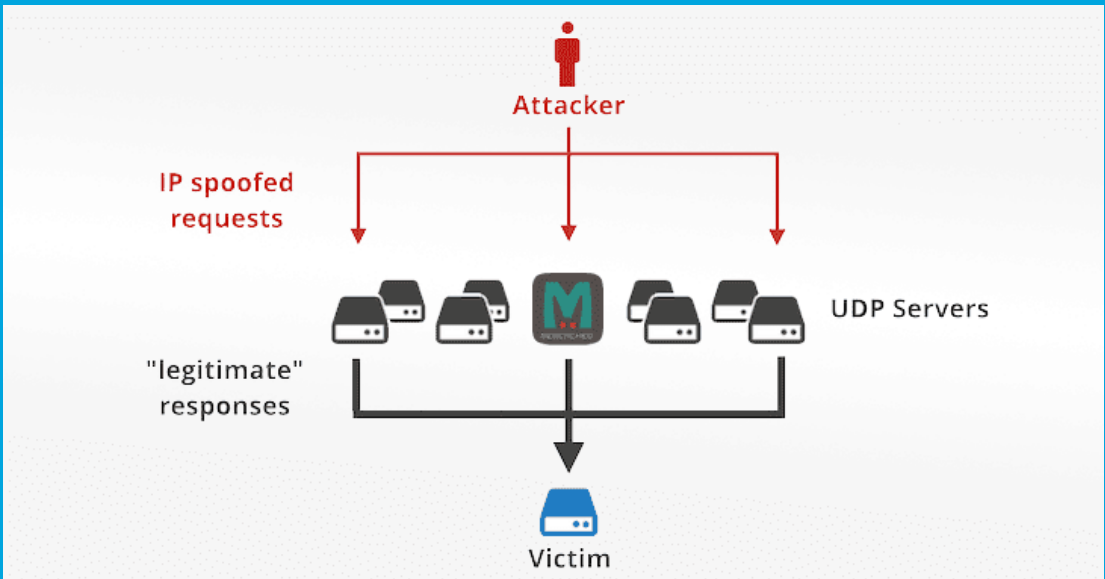
kindred

Security Newsletter

5 March 2018

Subscribe to this newsletter

Memcached Servers Can Be Abused for Insanely Massive DDoS Attacks



Cybercriminals have figured out a way to abuse widely-used Memcached servers to launch over 51,000 times powerful DDoS attacks than their original strength, which could result in knocking down of major websites and Internet infrastructure. In practice we've seen a 15 byte request result in a 750kB response (that's a 51,200x amplification). Memcached is a popular open-source and easily deployable distributed caching system that allows objects to be stored in memory and has been designed to work with a large number of open connections. Memcached server runs over TCP or UDP port 11211.

The general idea behind all amplification attacks is the same. An IP-spoofing capable attacker sends forged requests to a vulnerable UDP server. The UDP server, not knowing the request is forged, politely prepares the response. The problem happens when thousands of responses are delivered to an unsuspecting target host, overwhelming its resources. Amplification

attacks are effective, because often the response packets are much larger than the request packets. Thisn attacker with limited IP spoofing capacity (such as 1Gbps) to launch very large attacks (reaching 100s Gbps) "amplifying" the attacker's bandwidth.

New evidence suggests this novel attack method is fueling digital shakedowns in which victims are asked to pay a ransom to call off crippling cyberattacks. Cybereason, a Boston-based security company, said it has seen memcached attack payloads that consist of a simple ransom note requesting payment of 50 XMR (Monero virtual currency). Paying the Monero ransom won't help companies at all. That's because attackers have used the same Monero address for multiple DDoS attacks against different targets, they won't know who payed.

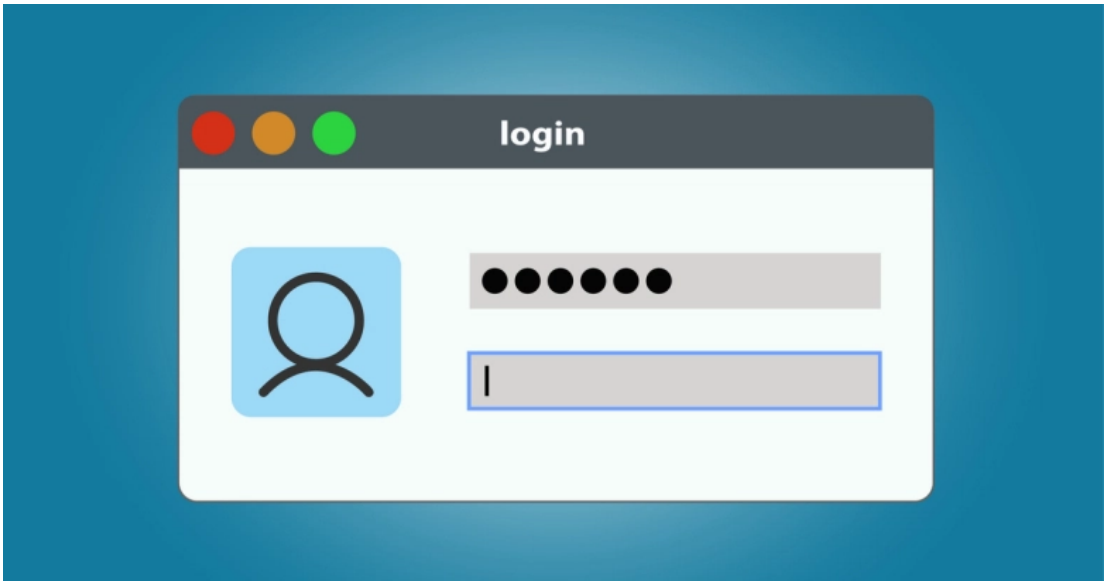
It's necessary to fix this and prevent further attacks. If you are using memcached, please disable UDP support if you are not using it. Please also ensure that your memcached servers are firewalled from the internet! Finally, developers: Please stop using UDP. If you must, please don't enable it by default. In order to defeat such attacks in future, we need to fix vulnerable protocols and also IP spoofing. As long as IP spoofing is permissible on the internet, we'll be in trouble.

Read More

Even More

Live attacks add extortion in Monero

Single Sign-On authentication – the SAML bug that lets you logon as someone else



Logon security company Duo recently found a rather worrying flaw in its own authentication gateway. A bit of digging revealed that the flaw was reflected in many other so-called single-sign on (SSO) applications, thanks to a problem in handling the underlying “authentication language” that has become a standard for products in this space.

This vulnerability can allow an attacker with authenticated access to trick SAML systems into authenticating as a different user without knowledge of the victim user’s password. In the vocabulary of SSO, network authentication uses dedicated authentication servers, known as IdPs (Identity Providers), to validate requests from client software (users) for access to servers on the network, known as SPs (service providers). This means that you don’t need to program an authentication module, or maintain a separate password database, or run yet another two-factor authentication service, for every server.

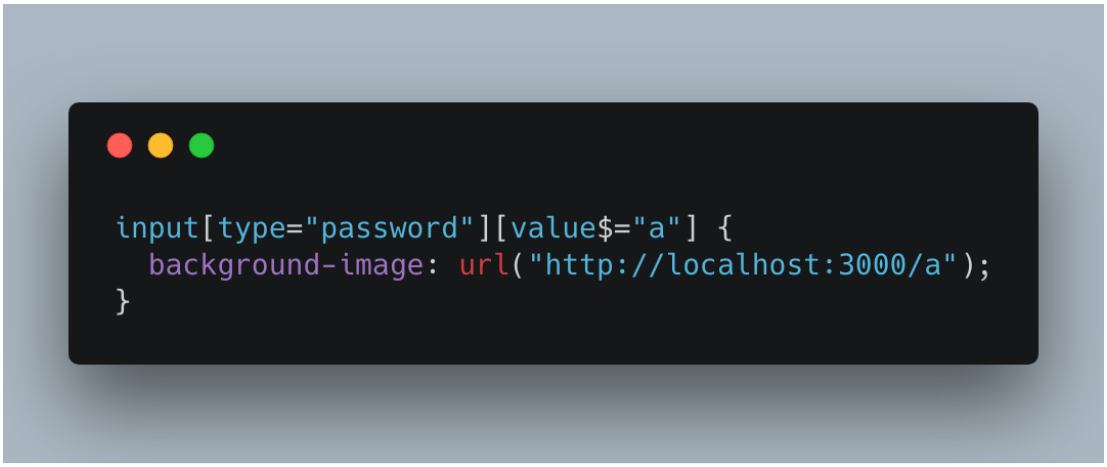
It is recommended that individuals that rely on SAML-based SSO to update any affected software to patch this vulnerability. The presence of this behavior is not great, but not always exploitable. SAML [identity providers] and [service providers] are generally very configurable, so there is lots of room for increasing or decreasing impact," the Duo Labs team says. Researchers recommend disabling public registration of user accounts on sensitive networks and vetting each user manually to avoid attackers registering an account on internal networks in the first place. If this is not possible, network admins can configure a whitelist of accepted email address domain names to limit who can register on the network, albeit this is not a reliable protection measure and a determined attacker will find a way around it. The attack is not possible against accounts protected by two-factor authentication (2FA) solutions.

Read More

Even More

Technical details

Third party CSS is not safe



A few days ago there was a lot of chatter about a 'keylogger' built in CSS. Some folks called for browsers to 'fix' it. Some folks dug a bit deeper and saw that it only affected sites built in React-like frameworks, and pointed the finger at React. But the real problem is thinking that third party content is 'safe'.

If you're including script from another origin, you must absolutely trust them, and their security. If you get hit by a bad script, you should purge all site data using the Clear-Site-Data header. CSS is much closer in power to a script than an image. Like a script, it applies to the whole page. CSS can't modify origin storage, and you can't build a cryptocoin miner in CSS (probably, maybe, I don't know), but malicious CSS can still do a lot of damage. As explained above, they can be used to make a keylogger in certain conditions. They can also be leveraged to make content disappear, add new content or move existing one, etc.

Third party content has a high impact within its sandbox. An image or a sandboxed iframe has a pretty small sandbox, but script & style are scoped to your page, or even the whole origin. If you're worried about users tricking your site into loading third party resources, you can use CSP as a safety net, to limit where images, scripts and styles can be fetched from. You can also use Subresource Integrity to ensure the content of a script/style matches a particular hash, otherwise it won't execute.

Read More

CSS Keylogger PoC

Can the FBI really unlock any iPhone?

US media giant Forbes is making a bold claim: the Feds can now unlock every iPhone in existence. The company that caused Forbes to make this dramatic claim is Cellebrite. You may recall that the FBI famously broke into the iPhone 5C of the dead San Bernadino terrorist and mass murderer Syed Rizwan Farook. In the end, it seems that Cellebrite helped out in the San Bernadino case, in a phone hack that involved a system that worked only on a “narrow slice of phones,” apparently including the iPhone 5C but not the iPhone 5s or later.

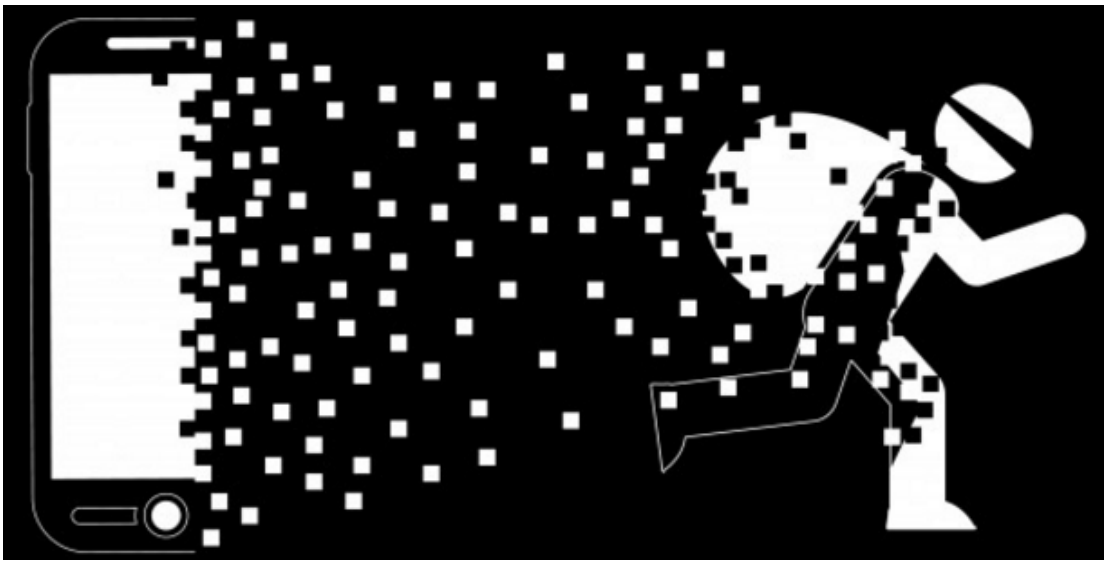
Now, if Forbes is to be believed, Cellebrite has extended the range of phones it can successfully unlock, including any iOS device running iOS5 to iOS11. According to Bruce Schneier, rumors are that Cellebrite hires ex-Apple engineers and moves them to countries where Apple can't prosecute them under the DMCA or its equivalents. There's also a credible rumor that Cellebrite's mechanisms only defeat the mechanism that limits the number of password attempts. It does not allow engineers to move the encrypted data off the phone and run an offline password cracker. If this is true, then strong passwords are still secure.

Let’s assume the worst – namely that Cellebrite does have a pair of iPhone and Android zero-day aces in the hole. You can bet your boots that Cellebrite will go many miles out of its way not to let those zero-days become known, because they’re the geese that lay the golden purchase orders. So, even if Cellebrite is willing to have a go at cracking phones, for a fee, your device still isn’t wide open to just anyone. If you think you could be the target to such services, patch early, patch often, use the longest phone lock code you can manage with the shortest lock period you can tolerate.

Read More

Even More

How to Fight Mobile Number Port-out Scams



T-Mobile, AT&T and other mobile carriers are reminding customers to take advantage of free services that can block identity thieves from easily “porting” your mobile number out to another provider, which allows crooks to intercept your calls and messages while your phone goes dark. Tips for minimizing the risk of number porting fraud are available below for customers of all four major mobile providers, including Sprint and Verizon.

Unauthorized mobile phone number porting is not a new problem, but T-Mobile said it began alerting customers about it earlier this month because the company has seen a recent uptick in fraudulent requests to have customer phone numbers ported over to another mobile provider’s network. Crooks typically use phony number porting requests when they have already stolen the password for a customer account (either for the mobile provider’s network or for another site), and wish to intercept the one-time password that many companies send to the mobile device to perform two-factor authentication.

Bigger picture, these porting attacks are a good reminder to use something other than a text message or a one-time code that gets read to you in an automated phone call. Whenever you have the option, choose the app-based alternative: Many companies now support third-party authentication apps like Google Authenticator and Authy, which can act as powerful two-factor authentication alternatives that are not nearly as easy for thieves to intercept.

Read More

Cutting room floor

- Introducing the Adversary Resilience Methodology — Part Two
- Unprotected AWS Bucket Exposes 50.4 GB of Financial Giant's Data
- 23,000 HTTPS certs will be axed in next 24 hours after private keys leak
- Dear developers, beware of DNS Rebinding
- New RedDrop Android Spyware Records Nearby Audio
- Implement "security.txt" to advocate responsible vuln. disclosures
- An argument for passwordless
- Why your company should consider implementing DNS security extensions
- https://medium.com/bugbountywriteupInfosec Writeups:A collection of medium posts around bug bounties, CTFs, vulnhub machines, etc.
- RIP CERT.org – You Will Be Missed

#Tech and #Tools

- Guide to using YubiKey as a SmartCard for GPG and SSH
- CSS-Keylogger Proof of Concept
- Honeytrap: Open-source framework for honeypots.
- Bettercap 2.0: Advanced Man in the Middle Attack Framework
- Checks Firefox saved passwords against the Have I Been Pwned API. #UseAtYourOwnRisks
- dotdotslash: Search for Directory Traversal Vulnerabilities
- New bypass and protection techniques for ASLR on Linux
- Kali Linux 2018.1 Release
- OWASP DependencyCheck: Detects publicly disclosed vulnerabilities in application dependencies.
- Default Password database
- CVE-2018-4087 PoC: Escaping the sandbox by misleading bluetoothd
- The infamous issue of target _blank code
- FinFisher exposed: A researcher's tale of defeating traps, tricks, and complex virtual machines
- Paseto is a Secure Alternative to the JOSE Standards (JWT, etc.)

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 over 15 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 13 subsidiaries and 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 as an innovation driven company that builds on trust.

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