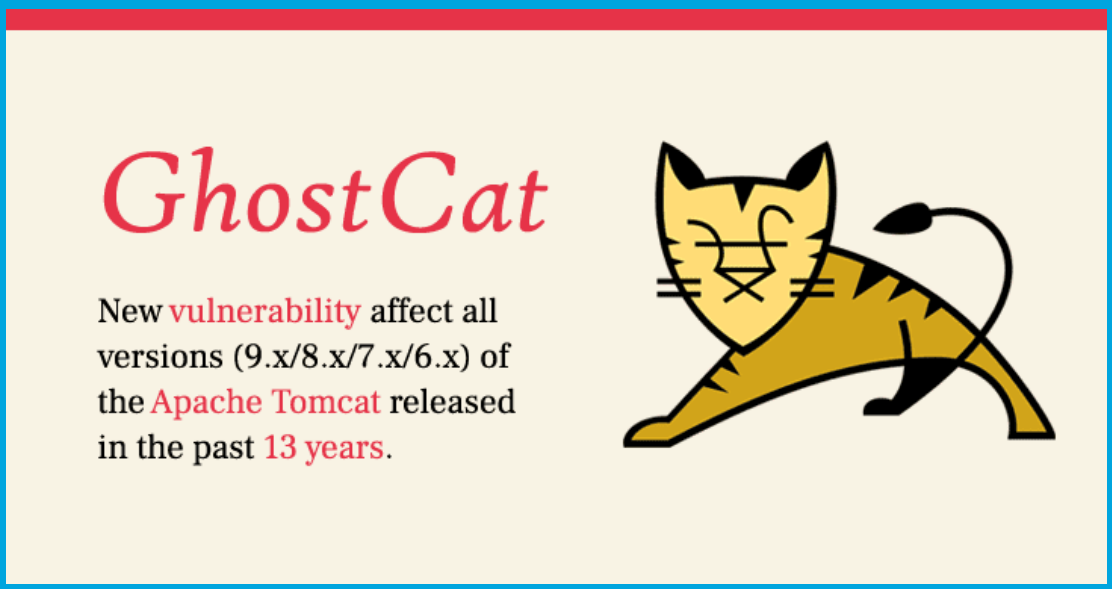
Security Newsletter

2 March 2020

Subscribe to this newsletter

GhostCat: New High-Risk Vulnerability Affects Servers Running Apache Tomcat



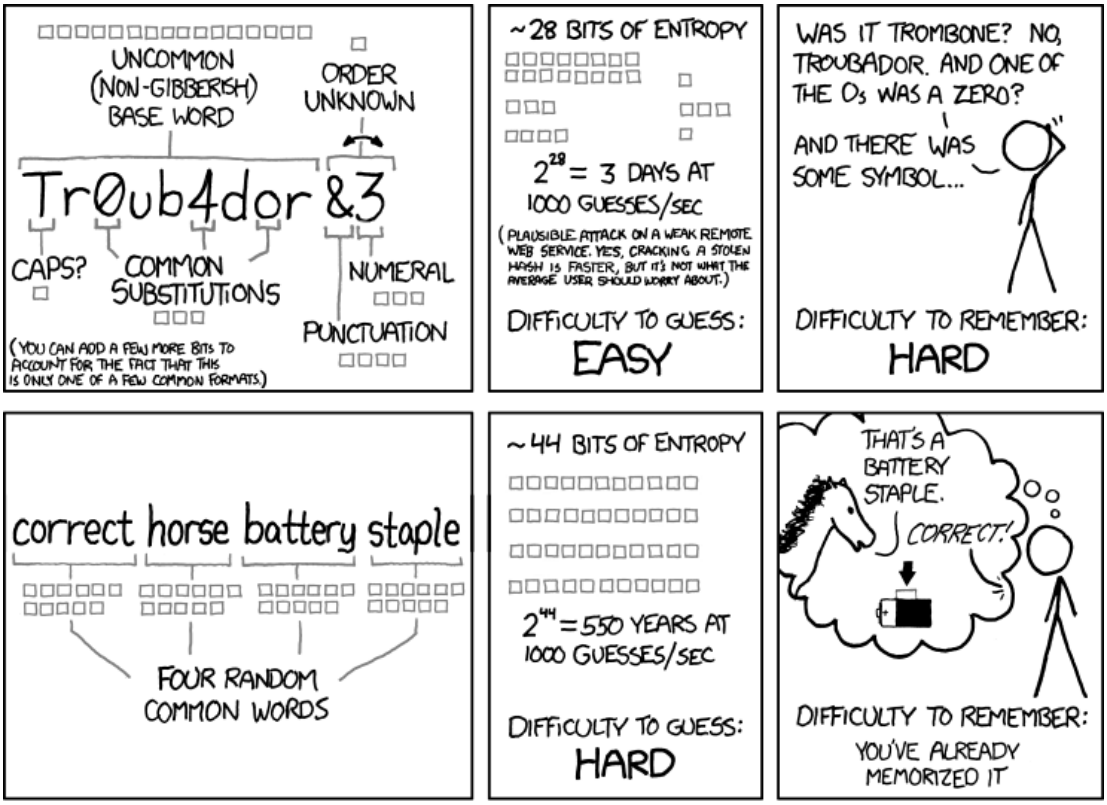
If your web server is running on Apache Tomcat, you should immediately install the latest available version of the server application to prevent hackers from taking unauthorized control over it. Yes, that's possible because all versions (9.x/8.x/7.x/6.x) of the Apache Tomcat released in the past 13 years have been found vulnerable to a new high-severity (CVSS 9.8) 'file read and inclusion bug'—which can be exploited in the default configuration.

But it's more concerning because several proof-of-concept exploits for this vulnerability have also been surfaced on the Internet, making it easy for anyone to hack into publicly accessible vulnerable web servers. Dubbed 'Ghostcat' and tracked as CVE-2020-1938, the flaw could let unauthenticated, remote attackers read the content of any file on a vulnerable web server and obtain sensitive configuration files or source code, or execute arbitrary code if the server allows file upload, as shown in a demo below.

Chaitin researchers found and reported this flaw last month to the Apache Tomcat project, who has now released Apache Tomcat 9.0.31, 8.5.51, and 7.0.100 versions to patch the issue. Web administrators are strongly recommended to apply the software updates as soon as possible and advised to never expose AJP port to untrusted clients because it communicates over the insecure channel and meant to be used within a trusted network. However, if, for some reason, you can't upgrade your affected web server immediately, you can also disable the AJP Connector directly, or change its listening address to the localhost.

Read More on TheHackerNews

FBI recommends passphrases over password complexity



"Instead of using a short, complex password that is hard to remember, consider using a longer passphrase," the FBI said. "This involves combining multiple words into a long string of at least 15 characters," it added. "The extra length of a passphrase makes it harder to crack while also making it easier for you to remember."

The idea behind the FBI's advice is that a longer password, even if relying on simpler words and no special characters, will take longer to crack and require more computational resources. Even if hackers steal your encrypted password from a hacked company, they won't have the computing power and time needed to crack the password. Academic research published in 2015 supports this argument, explaining that "the effect of increasing the length dwarfs the effect of extending the alphabet [adding complexity]."

Furthermore, NIST password recommendations issued in 2017 have also urged websites and web services to accommodate longer password fields of up to 64 characters for this same reason -- to let users choose passphrases instead of short passwords. The same NIST guideline also recommended using passphrases over passwords when possible.

Read More on ZDNet

More #News

- Let's Encrypt Issued A Billion Free SSL Certificates in the Last 4 Years
- FBI Says $140+ Million Paid to Ransomware, Offers Defense Tips
- Facial recognition company Clearview AI hit by data theft
- 92% of Americans would delete an app that sold their personal information
- Hackers Use Windows 10 RDP ActiveX Control to Run Griffon Backdoor
- 49 Million Unique Emails Exposed Due to Mishandled Credentials
- Microsoft Edge Now Lets You Block Potentially Unwanted Programs
- 11 things you might not know about security operations center burnout
- Slickwraps data breach earns scorn for all
- Android malware can steal Google Authenticator 2FA codes
- Credit Card Skimmer Uses Fake CDNs To Evade Detection
- New LTE Network Flaw Could Let Attackers Impersonate 4G Mobile Users
- Newly Declassified Study Demonstrates Uselessness of NSA's Phone Metadata Program
- 18 Sniffers Steal Payment Card Data from Print Store Customers
- uBlock Origin 1.25 Now Blocks Cloaked First-Party Scripts, Firefox Only
- KrØØk: Serious vulnerability affected encryption of billion+ Wi–Fi devices

#Patch Time!

- Mystery zero-day in Chrome – update now!
- Cisco Working on Patches for New Kr00k WiFi Vulnerability
- Adobe fixes critical flaws in Media Encoder and After Effects
- NVIDIA Fixes High Severity Flaw in Windows GPU Display Driver
- Critical Bugs in WordPress Plugins Let Hackers Take Over Sites
- Hackers Scanning for Vulnerable Microsoft Exchange Servers, Patch Now!

#Tech and #Tools

- CVE-2020-1938: GhostCat
- The Detection Spectrum
- Using your devices as the key to your apps
- Windows persistence via shims
- Finding Pwned Passwords in Active Directory
- Torture-Proof Authentication
- Silver & Golden Tickets
- Other Security Features of Content Security Policy
- Sigma: Generic Signature Format for SIEM Systems
- Defeating a Laptop's BIOS Password
- Pass the Hash
- Chepy: Python lib/cli equivalent of the awesome CyberChef tool
- Getting What You're Entitled To: A Journey Into MacOS Stored Credentials
- RedELK: Red Team's SIEM - tracking and alarming about Blue Team activities

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