kindred

Security Newsletter

4 June 2018

Subscribe to this newsletter

Kingred Group is growing, so does the Group Security team! We're looking for new talented professionals to come join us:

- You like to break things, then explain how to fix it? Be part of our Cyber Security team
- You prefer the blue team side? Check out our SOC analyst position
- You're into identity and access management? We are looking for an IAM Specialist
- Interested in Governance, Risk and Compliance? Apply for our InfoSec team

Kindred is one of the largest online gambling companies in the world with over 15 million customers across 100 markets. You can find all our open vacancies on our career page.

Git users: Update now to avoid massive remote code execution flaw

A recently revealed flaw in Git could allow an attacker to execute arbitrary remote code by infecting a Git project. The exploit, assigned a Common Vulnerabilities and Exposures (CVE) number of CVE-2018-11235, is triggered when users recursively clone repositories that contain a malicious .gitmodules file. The exploit essentially functions like a directory traversal attack that uses .gitmodules files as its starting point.

Git is a popular version control platform for software development that simplifies change tracking and collaboration. Git repositories can be hosted locally, or platforms like GitHub can be used to store code in the cloud.

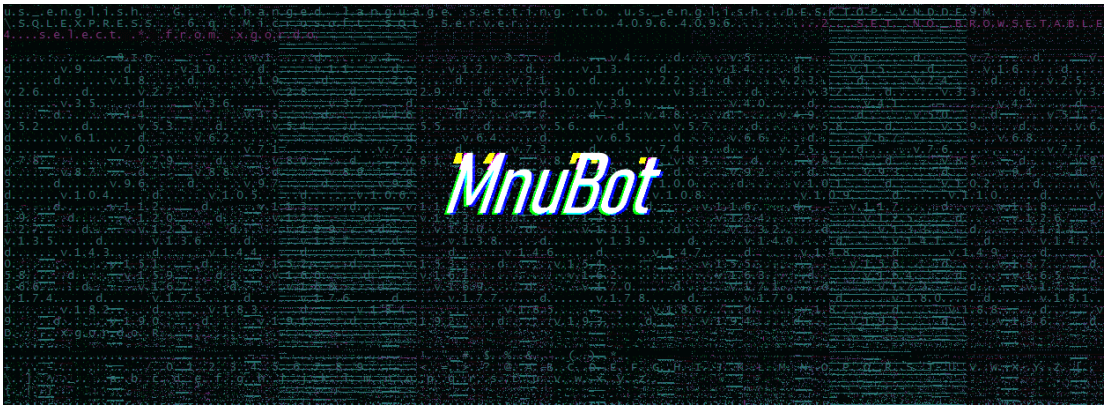
The exploit, according to the NIST National Vulnerability Database, affects all versions of Git "before 2.13.7, 2.14.x before 2.14.4, 2.15.x before 2.15.2, 2.16.x before 2.16.4, and 2.17.x before 2.17.1.".

There isn't much action for users or administrators to take to solve this issue outside of updating their Git platforms as soon as a new version is published. Don't wait on this fix—the alternative could be devastating. But patches aren't only rolled out to Git clients. A fix is also included for Git's server-side component.

Even More

Read More

MnuBot Banking Trojan Tries to Hide Behind MSSQL Traffic



Security researchers have spotted a new banking trojan named MnuBot that uses some atypical tricks to avoid easy detection on compromised hosts. Discovered by the IBM security team, this trojan is written in Delhpi, and its author is currently spreading it to Brazilian targets only. But while most Delphi-based malware is generally considered as unsophisticated, MnuBot got the IBM team's interest due to an odd trick it used to disguise its traffic.

According to Jonathan Lusky, a malware researcher for IBM Security's Trusteer's group, this new banking trojan is controlled by crooks via a remote Microsoft SQL (MSSQL) database. All communications between the malware and its C&C server occurs as SQL traffic. This includes queries for new commands, and the commands themselves.

Like many other malware families in the region, MnuBot uses a full-screen overlay form to assist the attacker to commit the fraud. Overlaying forms are used to prevent the victims from accessing their open banking session inside the browser. Those forms are a type of social engineering to keep the user waiting. In the background, the cybercriminal takes control over the user endpoint and attempts to perform an illegal transaction via the victim’s open banking session.

Read More

Even More

Cutting room floor

- Your logo and branded vulnerability aren't helping: How to disclose better
- Ghostery Tries to Comply With GDPR, but Ends Up Violating GDPR in the Process
- What is Shodan? The search engine for everything on the internet
- Valve Patches 10-Year Old Flaw in Steam Client
- GDPR vs. ePrivacy: The 3 differences you need to know
- HTTP Parameter Pollution Leads to reCAPTCHA Bypass
- Remote Code Execution Vulnerability Disclosed in Windows JScript Component
- Hundreds of Android devices shipped with pre-installed malware
- Coca-Cola Suffers Breach at the Hands of Former Employee

#Tech and #Tools

- IVRE: Open-source framework for network recon.
- PassProtect: Stop using bad passwords.
- Side-channel attacking browsers through CSS3 features
- How to rotate your Twitter API key and bearer token automatically with AWS Secrets Manager
- SteamClient RCE details
- BackSwap malware finds innovative ways to empty bank accounts
- QRadar Remote Command Execution
- ReCaptcha Bypass by HTTP parameter pollution

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