kindred

Security Newsletter

13 August 2018

Subscribe to this newsletter

How I gained commit access to Homebrew in 30 minutes

"Since the recent NPM, RubyGems, and Gentoo incidents, I've become increasingly interested, and concerned, with the potential for package managers to be used in supply chain attacks to distribute malicious software. Specifically with how the maintainers and infrastructure of these projects can be targeted as an attack vector. On Jun 31st, I went in with the intention of seeing if I could gain access to Homebrew's GitHub repositories. About 30 minutes later, I made my first commit to Homebrew/homebrew-core."

GitHub Support was contacted and they verified the relevant token had not been used to perform any pushes to Homebrew/brew or Homebrew/homebrew-core during the period of elevated scopes. To be explicit: no packages were compromised and no action is required by users due to this incident.

If you're a Brew user, there's no need for alarm and no immediate action you need to take. Holmes disclosed this responsibly to the Homebrew crew, who fixed the issue right away – within a few hours, in fact – and published a short, frank and informative disclosure notice. As in the case of Gentoo's recent supply-chain breach, the disclosure notice is worth reading whether the incident directly affects you or not. Supply-chain attacks can have wide-reaching effects, so ask yourself, "What can I and my own organisation learn from this?"

Read More

Even More

Homebrew statement

Cutting room floor

- Flaw in BIND Security Feature Allows DoS Attacks
- DarkHydrus Relies on Open-Source Tools for Phishing Attacks
- New WhatsApp Vulnerability Allows Hackers to Intercept and Change Message Contents
- DevSecOps: The Keys to Success
- How evil JavaScript helps attackers tag possible victims – and gives away their intent
- Snapchat Hack — Hacker Leaked Snapchat Source Code On GitHub
- Let’s Encrypt Root Certificate Now Directly Trusted by Microsoft and all Major Root Programs
- Pentagon bans military from using GPS apps and fitness trackers
- Top tip? Sprinkle bugs into your code to throw off robo-vuln scanners
- Facebook releases Fizz: TLS 1.3 library
- TSMC Chip Maker Blames WannaCry Malware for Production Halt
- Mastering MITRE's ATT&CK Matrix
- New Method Simplifies Cracking WPA/WPA2 Passwords on 802.11 Networks
- Hundreds of HP inkjet printer models vulnerable to critical remote code execution flaws
- Numerous OpenEMR Security Flaws Found; Most Patched
- Windows 10 to get disposable sandboxes for dodgy apps

#Tech and #Tools

- Netflix Cloud Security: Detecting Credential Compromise in AWS
- BloodHound 2.0
- Hunting with JA3
- GitRob: Reconnaissance tool for GitHub organizations
- GitLeaks: Audit git repos for secrets 🔑
- How to use reverse DNS records to identify mass scanners
- Practical Web Cache Poisoning
- How to DoH (DNS over HTTPS) only with Firefox
- Protecting internal applications with a SAML-aware reverse-proxy (a tutorial)
- Step: A New Zero Trust Swiss Army Knife from Smallstep
- A Linux Auditd rule set mapped to MITRE's Attack Framework
- When "ASLR" Is Not Really ASLR - The Case of Incorrect Assumptions and Bad Defaults
- PIN analysis

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