Security Newsletter

18 February 2019

Subscribe to this newsletter

RunC Flaw Lets Attackers Escape Linux Containers to Gain Root on Hosts

A serious security vulnerability has been discovered in the core runC container code that affects several open-source container management systems, potentially allowing attackers to escape Linux container and obtain unauthorized, root-level access to the host operating system.

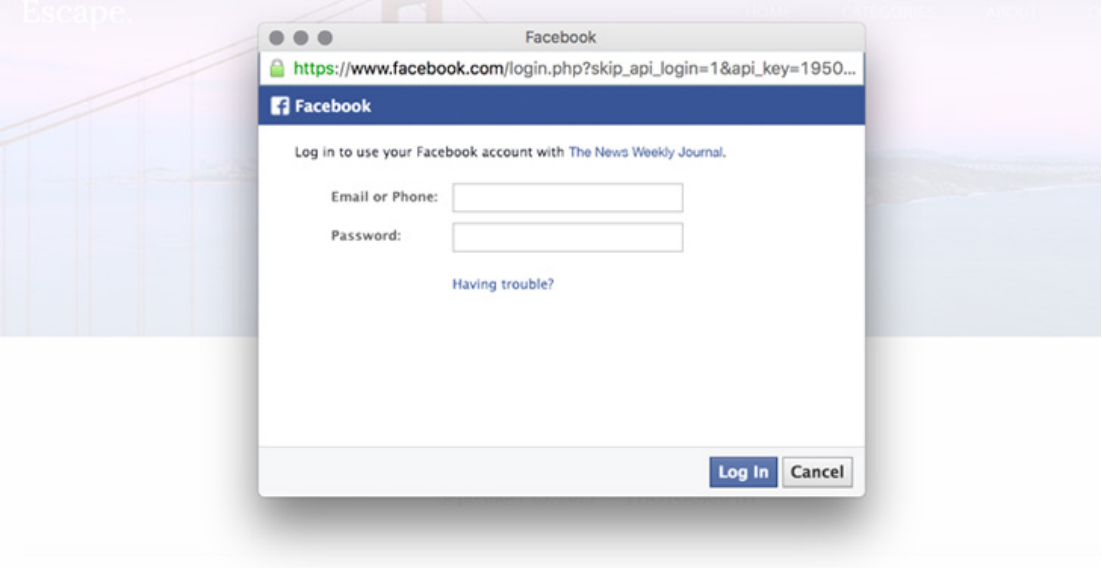
The flaw resides in runC—a lightweight low-level command-line tool for spawning and running containers, an operating-system-level virtualization method for running multiple isolated systems on a host using a single kernel. Originally created by Docker, runC is the default container run-time for Docker, Kubernetes, ContainerD, CRI-O, and other container-dependent programs, and is widely being used by major cloud hosting and server providers.

A specially-crafted malicious container or an attacker having root access to a container could exploit this flaw (with minimal user interaction) to gain administrative privileges on the host machine running the container, eventually compromising the hundreds-to-thousands of other containers running on it. According to Red Hat, the vulnerability can be mitigated if SELinux in targeted enforcing mode is enabled, which is default on RedHat Enterprise Linux, CentOS, and Fedora.The maintainers of runC have published a git commit to resolving the security flaw, but all the projects built atop runC need to incorporate the patches in their products.

Read More on TheHackerNews

Even More on BankInfoSecurity

New Phishing Attack That Even Most Vigilant Users Could Fall For



How do you check if a website asking for your credentials is fake or legit to log in? By checking if the URL is correct? By checking if the website address is not a homograph? By checking if the site is using HTTPS? Or using software or browser extensions that detect phishing domains?

Well, if you, like most Internet users, are also relying on above basic security practices to spot if that "Facebook.com" or "Google.com" you have been served with is fake or not, you may still fall victim to a newly discovered creative phishing attack and end up in giving away your passwords to hackers.

Generally, when you click "log in with Facebook" button available on any website, you either get redirected to facebook.com or are served with facebook.com in a new pop-up browser window, asking you to enter your Facebook credentials to authenticate using OAuth and permitting the service to access your profile's necessary information. However, Vincent discovered that the malicious blogs and online services are serving users with a very realistic-looking fake Facebook login prompt after they click the login button which has been designed to capture users' entered credentials, just like any phishing site.

As shown in the video demonstration, the fake pop-up login prompt, actually created with HTML and JavaScript, are perfectly reproduced to look and feel exactly like a legitimate browser window—a status bar, navigation bar, shadows and URL to the Facebook website with green lock pad indicating a valid HTTPS. The only way to protect yourself from this type of phishing attack "is to actually try to drag the prompt away from the window it is currently displayed in. If dragging it out fails (part of the popup disappears beyond the edge of the window), it's a definite sign that the popup is fake."

Read More on TheHackerNews

Even More on Myki blog

More #News

- Microsoft: 70 percent of all security bugs are memory safety issues
- Windows Malware Runs on Macs, Bypasses Gatekeeper to Target Software Pirates
- Hackers Destroyed VFEmail Service – Deleted Its Entire Data and Backups
- Dunkin' Donuts accounts compromised in second credential stuffing attack in three months
- What comes after air gaps? DARPA asks world for ideas
- Hacker Breaches Dozens of Sites, Puts 127 Million New Records Up for Sale
- The Race to the Bottom of Credential Stuffing Lists; Collections #2 Through #5 (and More)
- Hacked versions of popular iOS games available on App Store
- Have tech companies taken two-factor authentication too far?
- Get-rich-quick social media scams are turning teens into money mules
- I was wrong about Google and Facebook: there's nothing wrong with them (so say we all)
- Use an 8-char Windows NTLM password? Don't. Every single one can be cracked in under 2.5hrs
- 500px.com breached

#Patch Time!

- Canonical Snapd Vulnerability Gives Root Access in Linux
- New macOS security flaw lets malicious apps steal your Safari browsing history
- Microsoft Patches PrivExchange Vulnerability in February Quarterly Updates
- Patch Tuesday, February 2019 Edition
- Researchers Implant "Protected" Malware On Intel SGX Enclaves
- Xiaomi electric scooters vulnerable to remote hijacking
- Dirty Sock vulnerability lets attackers gain root access on Linux systems

#Tech and #Tools

- OCTANE: Securize the exposure of web applications through cloud service provider
- Don't Give Me a Brake – Xiaomi Scooter Hack Enables Dangerous Accelerations and Stops for Unsuspecting Riders
- WebAuthn Development guide
- Evil Twin Attack: The definitive guide
- ENISA Training resources
- Runc and CVE-2019-5736
- Incident Response field manual
- Facebook CSRF protection bypass which leads to Account Takeover.
- Leaks_parser: Parser for data dumps Collection #1 / Collection #2-5
- Pwning wpa/wpa2 networks with bettercap and the pmkid client-less attack
- LNK & ISESteroids Powershell dropper

- CVE-2019-5736: runc container breakout (all versions)
- IoT Pentesting 101 && IoT security 101
- Autocert: Kubernetes automatic certificates
- WordPress Plugin 'Simple Social Buttons' Critical Security Bug

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 24 million customers across 100 markets. 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 as an innovation driven company that builds on trust.

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