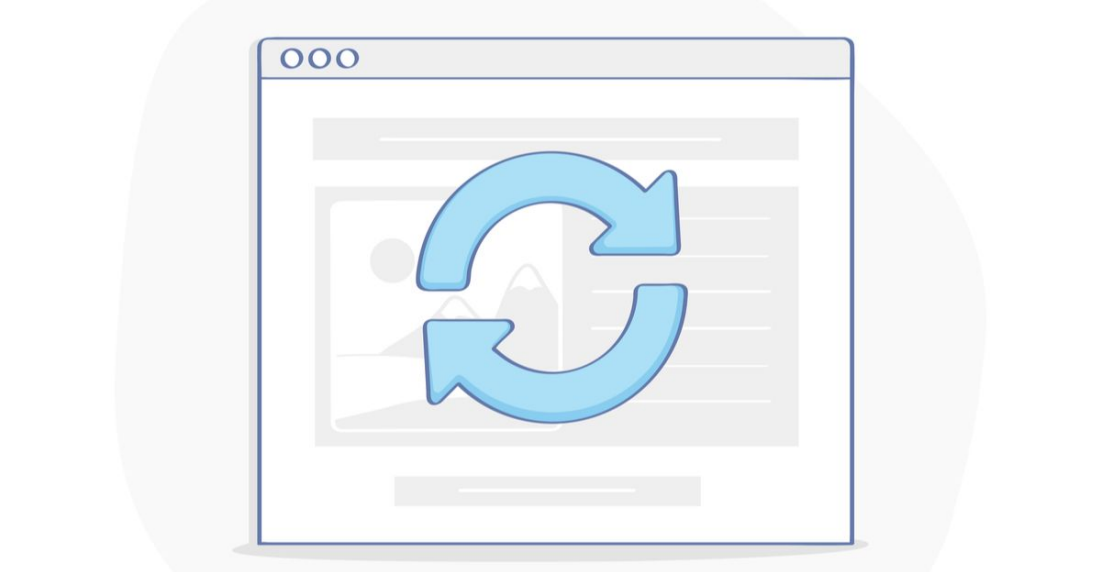
Security Newsletter

25 June 2018

Subscribe to this newsletter

It's time for TLS 1.0 and 1.1 to die, you may want to update your browser asap



TLS is the encryption on many of the internet protocols we use every day: for example, when we send authentication credentials and credit card information over the web, as well as for internet services such as email, FTP and VPN. As TLS 1.3 inches towards publication into the Internet Engineering Task Force's RFC series, it's a surprise to realise that there are still lingering instances of TLS 1.0 and TLS 1.1.

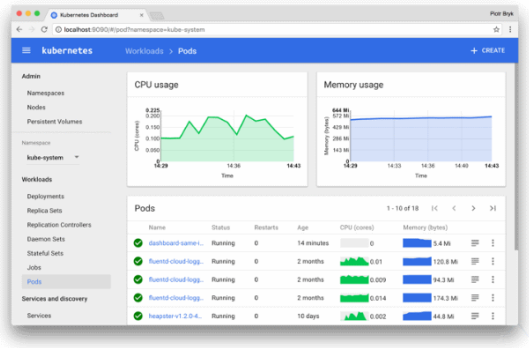
Online merchants have until 30 June to support TLS 1.2 and HTTP/1.1: a kill date that was extended for these security sadsack protocols from the original June 2016 deadline, which the PCI Council decided that retailers weren't going to make. Apart from websites, organisations like 3GPP 5G, CloudFlare, Amazon and GitHub have either completed their deprecation or will finish the job by July.

The council says that online and e-commerce environments using SSL and early TLS are the most susceptible to the SSL exploits, but the 30 June 2018 PCI DSS migration date applies to all environments except for payment terminals (POIs) (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits for SSL and early TLS. PayPal, for its part, put out a notice reminding merchants that they have to support TLS 1.2 and HTTP/1.1 by June 30: insecure connections will break after that.

Read More

Why you may want to update your browser in the next 5 days

Over 22,000 Container Orchestration Systems Connected to the Internet



The admin consoles of over 22,000 container orchestration and API management systems are currently exposed online, according to a report published on Monday by Lacework, a company specialized in cloud security. In its report, the company analyzed the breadth of the problem of cloud management systems left exposed online, focusing on container orchestration systems, such as Kubernetes, Docker Swarm, Mesos Marathon, Redhat Openshift, Portainer.IO, and Swarmpit.

"Although the vast majority of these management interfaces have credentials set up, there is little reason why they should be world-accessible and are far more vulnerable than they should be. These nodes are essentially openings to these organization's cloud environments to anyone with basic skills at searching the web. These organizations, and the others who will replicate their mistakes, are opening themselves up to brute force password and dictionary attacks."

The Lacework report, which also includes basic advice for avoiding such exposures and hardening container management panel security, highlights a growing trend in today's IT landscape where many system administrators appear to have forgotten what passwords, firewalls, and access control lists (ACLs) are good for.

Read More

LaceWork report on Containers at Risk

Cutting room floor

- Microsoft Edge Bug Exposes Content From Other Sites via HTML5 Audio Tag
- Finding phishing sites with CT
- Gaming Companies Remove Analytics App After Massive User Outcry
- Apple macOS Bug Reveals Cache of Sensitive Data from Encrypted Drives
- The new endpoint security market: Growing in size and scope
- Attackers Taking Over Insecure Cameras and Spying on Device Owners
- Cisco patches critical Nexus flaws: Are your switches vulnerable?
- Android Gets New Anti-Spoofing Feature to Make Biometric Authentication Secure
- ZeroFont Technique Lets Phishing Emails Bypass Office 365 Security Filters
- Popular Flight Tracker Flightradar24 Suffers Data Breach
- How to allow users to report suspicious emails with Outlook's Report Message feature
- OpenBSD Disables Intel Hyper-Threading to Prevent Spectre-Class Attacks
- Perverse Vulnerability from Interaction between 2-Factor Authentication and iOS AutoFill
- 'Olympic Destroyer' Malware Spotted in New Attacks
- New Azure password-banning tool will help kill off bad 'P@$$w0rd' habits

#Tech and #Tools

- Vendors, Disclosure, and a bit of WebUSB Madness
- Freedom Fighting Mode: open source hacking harness
- ProbeManager: Centralize Management of Intrusion Detection System like Suricata Bro Ossec ...
- Sandbagility: Framework to analyze malwares
- WireGuard: Fast, Modern, Secure VPN tunnel
- Graphical AES encryption tool for end users.
- ARPPD: An ARP Poisoning Defender script
- Containers and Cloud Security
- Technical details on Wavethrough vulnerability
- Reverse Shell from an OpenVPN Configuration File
- Attacking Private Networks from the Internet with DNS Rebinding
- Hiding in Plain Sight: Using the Office 365 Activities API to Investigate Business Email Compromises
- Tokenvator: A Tool to Elevate Privilege using Windows Tokens
- Cloud Exposure, DLP & IR, A-Z
- AWS Privilege Escalation – Methods and Mitigation
- Exploring PowerShell AMSI and Logging Evasion
- Advanced CORS Exploitation Techniques

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.

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