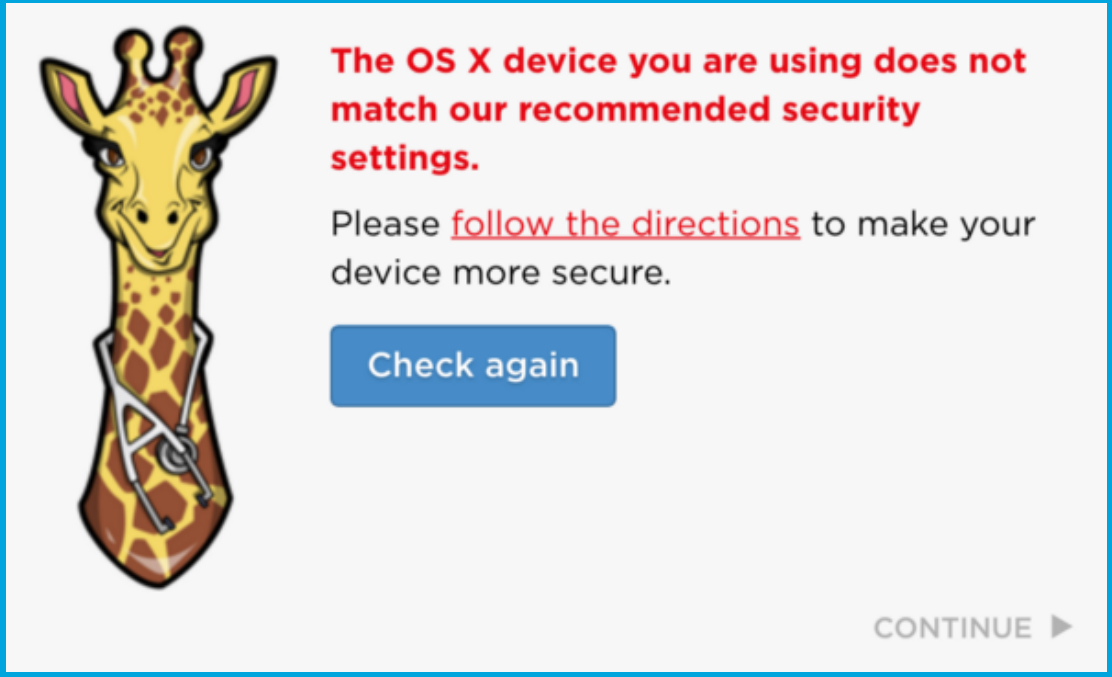
kindred

Security Newsletter

5 November 2018

Subscribe to this newsletter

Stethoscope: A user focused approach to endpoint health and management



Netflix announced the next big release in user focused security, the Stethoscope native app. The new native app includes basic device health recommendations with inline clickable instructions on how to update settings. It can also communicate with a web app (such as a Single Sign On provider) in order to make device health suggestions at pivotal moments.

TL;DR: Basic device hygiene is a fundamental security practice. People want to securely configure their devices, but they may not know what the best practices are, or how to comply with them. Empowering users to see the state of their devices and how to get them into an ideal state improves the overall security posture of an organization.

The Stethoscope app was built with not just device health in mind, but also with security in mind. The app does not run as root, and has no elevated privileges. The app does not change settings for users automatically. This respects the user's ownership of their device settings, but also has the benefit of not adding risk of settings being changed maliciously via the app. Device information can be sensitive, so we limited who is able to run scans. This is enforced via a CORS policy, which is configured at build time. The local server only listens on loopback so that device scans cannot be run outside of the local machine. Currently Mac OS and Windows 10 devices are supported.

Read More on Netflix Blog

Even More

Windows Built-in Antivirus Gets Secure Sandbox Mode – How To Turn It ON

Microsoft Windows built-in anti-malware tool, Windows Defender, has become the very first antivirus software to have the ability to run inside a sandbox environment.

Sandboxing is a process that runs an application in a safe environment isolated from the rest of the operating system and applications on a computer. So that if a sandboxed application gets compromised, the technique prevents its damage from spreading outside the closed area. Since antivirus and anti-malware tools run with the highest level of privileges to scan all parts of a computer for malicious code, it has become a desired target for attackers.

For now, Windows Defender running on Windows 10, version 1703 (also known as the Creators Update) or later, support the sandbox feature, which is not enabled by default, but you can turn the feature on by running some commands described in the article.

Read More on TheHackerNews

Read More on Microsoft Blog

More #News

- How one man could have taken over any business page on Facebook
- Apple's New MacBook Disconnects Microphone "Physically" When Lid is Closed
- Many CMS plugins are disabling TLS certificate validation... and that's very bad
- Technology preview: Sealed sender for Signal
- Now use Internet anonymously through Tor-enabled SIM card Onion3G
- Cathay Pacific breach exposes data of 9.4 million passengers
- Google won't let you sign in if you disabled JavaScript in your browser
- New Stuxnet Variant Allegedly Struck Iran
- Radisson Hotel Group Data Breach Exposed Customer's Personal Data

- Google's stealthy reCAPTCHA v3 detects humans – no questions asked
- Hackers Exploit Cisco Zero Day Vulnerability in Wild Resulting in DoS Condition
- Automating security at AWS: How Amazon Web Services operates with no SOC

#Patch Time!

- Twelve malicious Python libraries found and removed from PyPI
- Critical Code Execution Vulnerability Found in MKVToolNix Tools that Parses MKV Files
- Systemd: A nasty DHCPv6 packet can pwn a vulnerable Linux box
- Bleedingbit zero-day chip flaws may expose majority of enterprises to remote code execution attacks
- Update now! Apple releases security fixes for iOS, MacOS, Safari, others

#Tech and #Tools

- Kernel RCE caused by buffer overflow in Apple's ICMP packet-handling code (CVE-2018-4407)
- Persistent GCP backdoors with Google's Cloud Shell
- On-the-Run with Empire.
- For The Love of Money: Finding & Exploiting Vulnerabilities in Mobile Point of Sales Terminals
- Abusing PowerShell Desired State Configuration for Lateral Movement
- CVE-2018-9411: New critical vulnerability in multiple high-privileged Android services
- Trickbot Shows Off New Trick: Password Grabber Module
- Facebook Business Takeover
- Isolated Networks in the Cloud
- Tweetable Exploit for X.org Server Local Privilege Escalation (CVE-2018-14665) Released
- fuxploider: File upload vulnerability scanner and exploitation tool.
- Malware Sample Library #DontTryThisAtHomeOrWork
- Attacking Google Authenticator
- Covert Attack Mystery Box: A few novel techniques for exploiting Microsoft “features”
- Three C-Words of Web App Security: Part 2 – CSRF

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