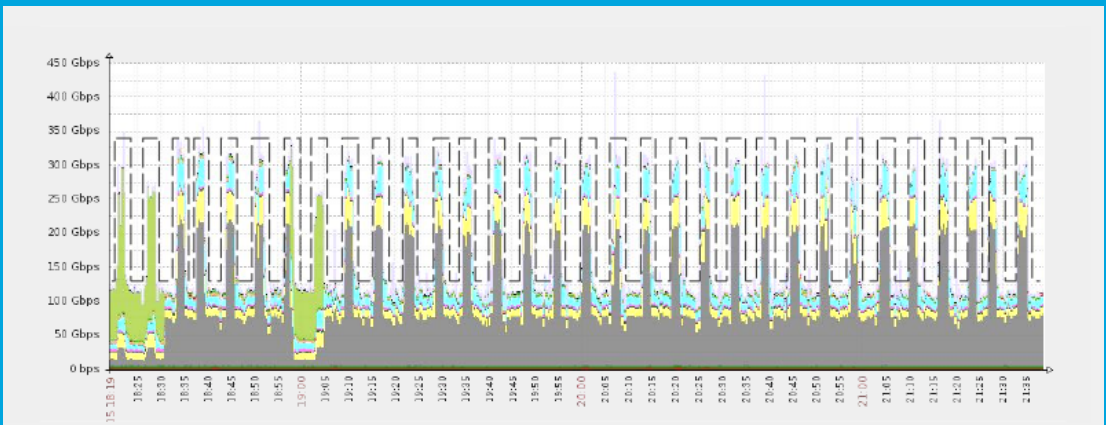
kindred

Security Newsletter

21 August 2017

Pulse Wave - New DDoS Assault Pattern Discovered



Pulse Wave DDoS Attack

A new method of carrying out DDoS attacks named Pulse Wave is causing problems to certain DDoS mitigation solutions, allowing attackers to down servers previously thought to be secured.

Classic attacks usually have the shape of a sloping triangle going up and down as an attacker slowly assembles bots and aims them at a desired target. The new pulse wave attacks start from zero and go to maximum values in a very short time span, then go back to zero, and back to maximum, repeating in continuous cycles at short clocked intervals.

Pulse wave attacks cause problems to hybrid mitigation solutions. The equipment and the targeted organization are shut down when one pulse hits. Recovering from one pulse usually takes a few minutes, by which time another pulse jams the network. Using this new technique, attackers can shut down organizations for extended periods of time, while also carrying out DDoS attacks on other targets.

Read More

Libsodium, the well-known cross-platforms cryptography library, got audited

Sodium is a modern, easy-to-use software library for encryption, decryption, signatures, password hashing and more. Its goal is to provide all of the core operations needed to build higher-level cryptographic tools.

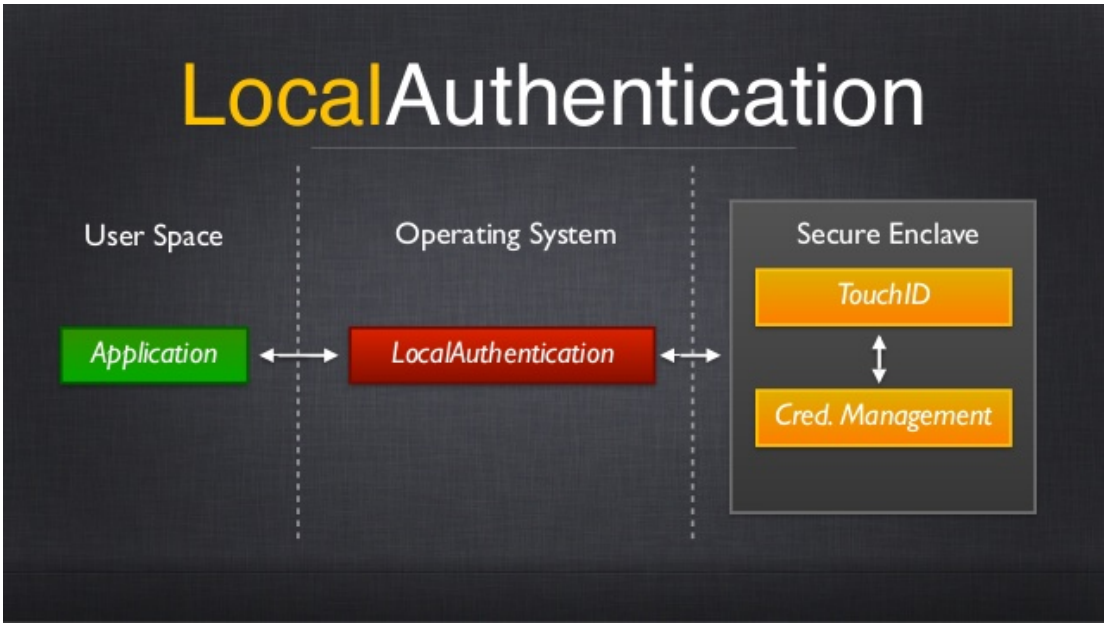
Private Internet Access today releases the results of its Libsodium audit. The Libsodium security assessment was conducted by Dr. Matthew Green of Cryptography Engineering on v1.0.12 and v1.0.13. Dr. Green previously completed the TrueCrypt audit with the Open Crypto Audit Project as well as an OpenVPN 2.4 audit on PIA's behalf.

The assessment found no critical flaws or vulnerabilities in the Libsodium library.

Read More

Audit Report

Hacker Releases Decryption Key for Apple's Secure Enclave Firmware



A hacker who goes online only by the pseudonym of Xerub has released the decryption key for Apple's Secure Enclave Processor (SEP) firmware.

The leak, confirmed by an Apple employee who wanted to remain anonymous, is crucial to iOS security, as it now allows hackers and security researchers alike access to a previously encrypted iOS component.

This key allows someone to decrypt the SEP firmware. It does not allow a third-party to decrypt and access TouchID or other data passing through SEP. Xerub's discovery is not inherently dangerous in itself, but through the ripples caused in the world of iOS security. A publicly available SEP decryption key will allow hackers, surveillance companies, and others to analyze and look for bugs in an area of iOS devices they previously had not had access to.

Read More

Even More

Unpatchable Flaw in Modern Cars Allows Hackers to Disable Safety Features

Researchers have discovered a security flaw that probably affects all new vehicles. It allows an attacker to turn off safety features, such as airbags, ABS brakes, and power-steering -- or any of a vehicle's computerized components connected to its controller area network or CAN bus.

Because it's a design flaw affecting the CAN bus messaging protocol standard used in CAN controller chips, the vulnerability can't simply be patched with a recall. It's also not specific to one vehicle model or its underlying electronics.

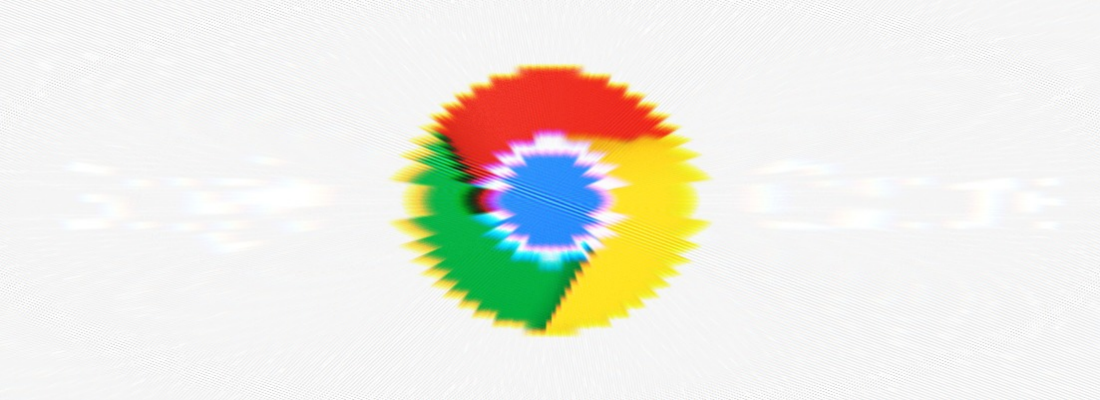
Initially developed in 1983 and put into production in 1989, the CAN standard manages the majority of the electrical subsystems and control units found in a significant number of modern smart cars.

By overloading the system with error messages, attackers can make a device to go into a Bus Off state, cutting it off from the greater CAN system and making it inoperable. The attack requires a "specially-crafted attack device" to be introduced via local access, which is only possible if the attacker has access to your vehicle.

Read More

Even More

RCE Vulnerability Affecting Older Versions of Chrome Will Remain Unpatched



A remote code execution vulnerability affects older versions of the Google Chrome browser, all except the current version — Chrome 60. To sum it up, the vulnerability is found in Google Chrome's Turbofan component, used to optimize JavaScript code.

In a response to the company's bug report, Google told Beyond Security engineers they do not plan to address the vulnerability because it does not work in the most recent version, the only one Google's security team is interested in servicing.

Exploiting the flaw requires luring a user to an attacker-controlled website and serving a piece of malicious JavaScript code. The flaw allows the attacker to execute code in the user's browser. While the vulnerability disclosure does not mention a sandbox escape to allow the attacker to execute code on the PC level, the flaw allows attackers to steal data accessible through the browser (cookies, passwords, etc.).

Google Chrome, overall, has a browser market share of around 59%. According to Web analytics firm Clicky, Chrome 60 accounts to 50% of those installations. This leaves nearly one in ten web users exposed to this flaw. Upgrading to the latest Chrome 60 version will mitigate this flaw.

Read More

Technical details

New NIST draft embeds privacy into US govt security for the first time

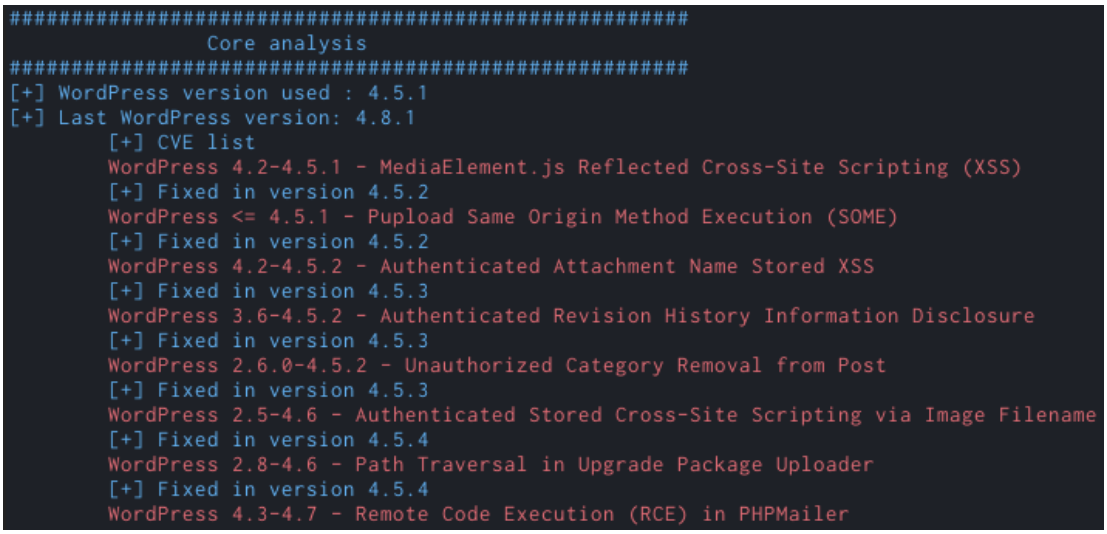
A draft of new IT security measures by the US National Institute of Standards and Technology (NIST) has for the first time pulled privacy into its core text as well as expanded its scope to include the internet of things and smart home technology.

Another interesting side effect of the new focus is that NIST has stopped pretending that it is only influencing federal agencies and is actively pitching its contents to private enterprise in the hope of building a more resilient overall network.

Among other things, it argues for a specific privacy program and separate privacy-focused training and includes two extensive appendices that track the privacy requirements and considerations for all the different named-and-numbered controls in the document.

Read More

CoMisSion – Whitebox CMS analysis



CoMisSion is a tool to automate all this stuff. You give it a CMS type (WordPress and Drupal are currently supported), a source code directory, an output filename and you are ready to go.

The tool prints its results to stdout. To gather CVEs, it uses the WPvulndb API. Once the version is identified, the tool downloads a « clean » archive of this version and checks for any alteration.

The tool generates a report as an XLSX file, with four tabs : The core; Alterations to the core; The plugins list and analyses; Alterations to plugins. This can be used as a starting point of a more in-depth audit.

Read More

Source Code

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.