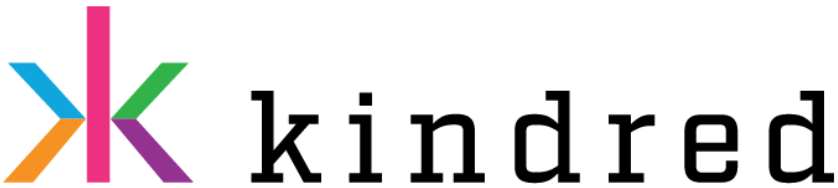
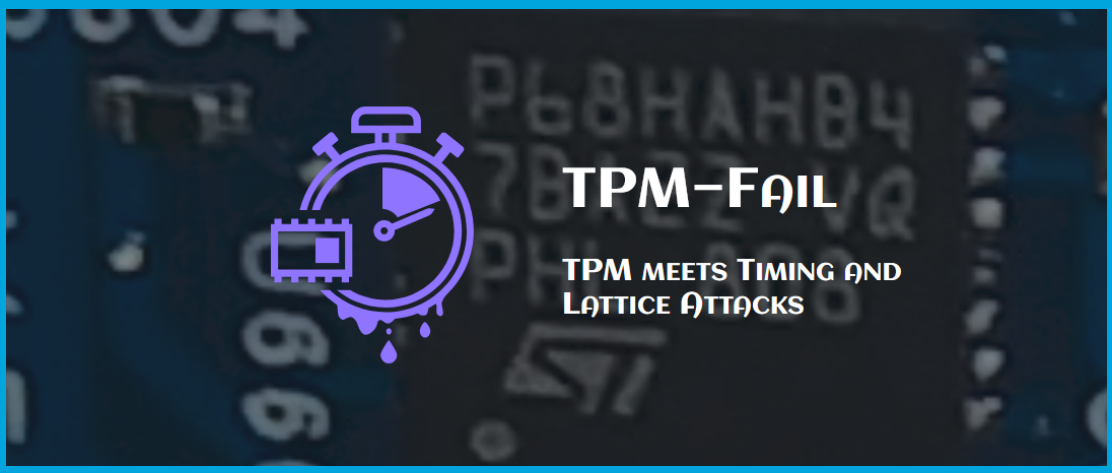


Security Newsletter

18 November 2019

Subscribe to this newsletter

TPM-FAIL vulnerabilities impact TPM chips in desktops, laptops, servers



A team of academics has disclosed today two vulnerabilities known collectively as TPM-FAIL that could allow an attacker to retrieve cryptographic keys stored inside TPMs. TPM stands for Trusted Platform Module. In the early days of computing, TPMs were separate chips added to a motherboard were a CPU would store and manage sensitive information such as cryptographic keys. These keys were used to ensure hardware integrity during the boot-up process or to attest various cryptographic operations, such as handling digital certificates, ensuring HTTPS connections on servers, or verifying authentication-related processes.

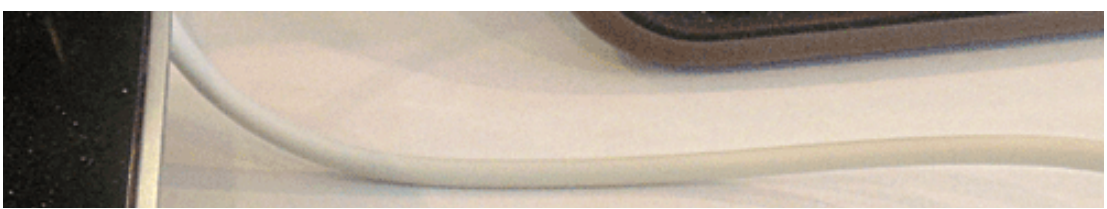
The actual attacks on these two TPM technologies is what security researcher call a "timing leakage." An external observer can record the time differences when the TPM is performing repetative operations and infer the data being processed inside the secure chip -- all based on the amount of time the TPM takes to do the same thing over and over again. The research team says the "timing leakage" they discovered can be used to extract 256-bit private keys that are being stored inside the TPM.

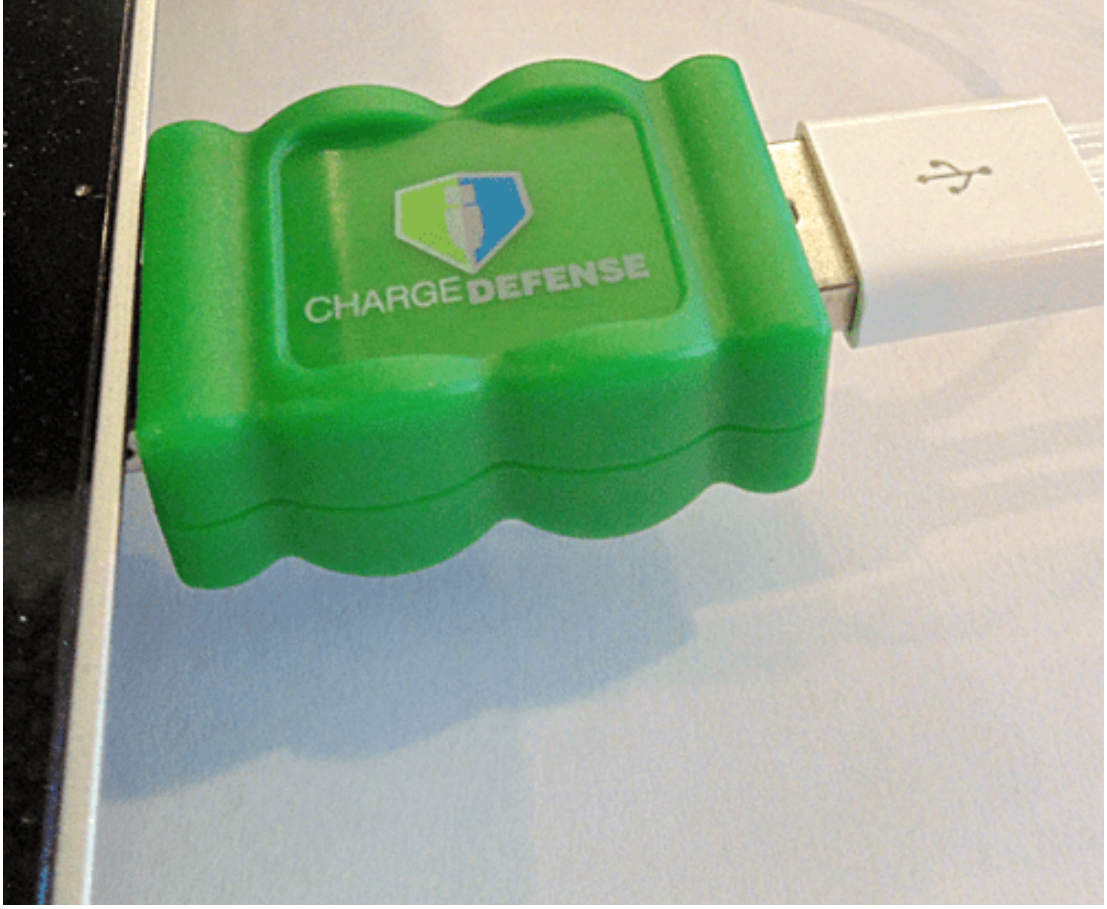
Both companies issued patches for the TPM-FAIL vulnerabilities, either by releasing security patches or by issuing new TPM chips. Intel upgraded their fTPM firmware to fix the security issue tracked as CVE-2019-11090 and STMicroelectronics issuing a new TPM chip to address the CVE-2019-16863 vulnerability, chips resistant against TPM-FAIL exploitation as the research team confirmed.

Read More on ZDNet

Even More on Bleeping Computer

Officials warn about the dangers of using public USB charging stations





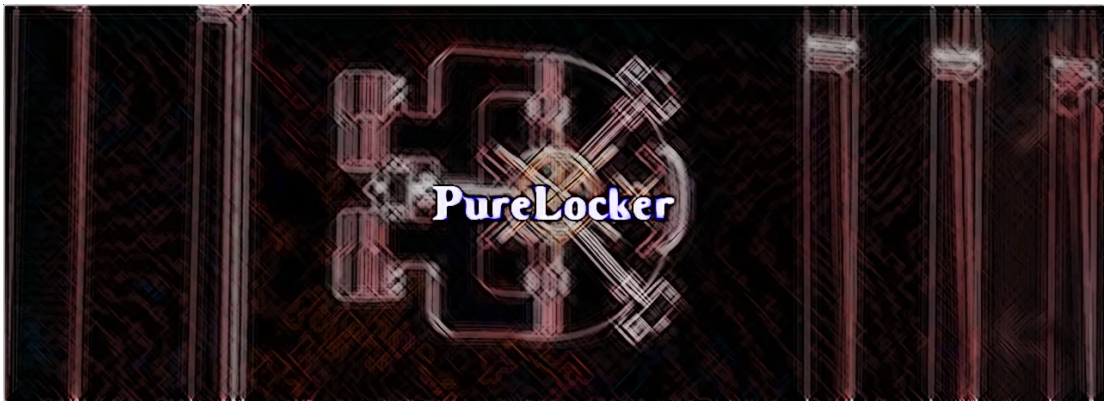
Travelers are advised to avoid using public USB power charging stations in airports, hotels, and other locations because they may contain dangerous malware, the Los Angeles District Attorney said in a security alert published last week. USB connections were designed to work as both data and power transfer mediums, with no strict barrier between the two. As smartphones became more popular in the past decade, security researchers figured out they could abuse USB connections that a user might think was only transferring electrical power to hide and deliver secret data payloads. This type of attack received its own name, as "juice jacking."

The LA District Attorney's warning [PDF] covers many attack vectors, because there's different ways that criminals can abuse USB wall chargers.The most common way is via "pluggable" USB wall chargers. These are portable USB charging devices that can be plugged into an AC socket, and criminals can easily leave some of these behind "by accident" in public places, at public charging stations. There are also USB chargers encased directly inside power charging stations installed in public places, were the user only has access to a USB port. However, LA officials say criminals can load malware onto public charging stations, so users should avoid using the USB port, and stick to using the AC charging port instead.

Taking all these into account, LA officials recommend that travelers: Use an AC power outlet, not a USB charging station. Take AC and car chargers for your devices when traveling. Consider buying a portable charger for emergencies. But there are also other countermeasures that users can deploy. One of them is that device owners can buy USB "no-data transfer" cables, where the USB pins responsible for the data transfer channel have been removed, leaving only the power transfer circuit in place. Such cables can be found on Amazon and other online stores.

Read More on ZDNet

PureLocker Ransomware Can Lock Files on Windows, Linux, and macOS



Cybercriminals have developed ransomware that can be ported to all major operating systems and is currently used in targeted attacks against production servers. The new name is PureLocker. Malware researchers analyzed samples for Windows but a Linux variant is also being used in attacks. The name of the ransomware derives from the programming language it's written in, PureBasic, an unusual choice that provides some benefits, "AV vendors have trouble generating reliable detection signatures for PureBasic binaries. In addition, PureBasic code is portable between Windows, Linux, and OS-X, making targeting different platforms easier."

The malware is carefully designed to evade detection, hiding malicious or dubious behavior in sandbox environments, posing as the Crypto++ cryptographic library, and using functions normally seen in libraries for music playback. For instance, if the malware determines that it's running in a debugger environment, it exits straight away. Furthermore, the payload deletes itself after execution. This and more allowed PureLocker to stay under the radar for months in a row. For the past three weeks, PureLocker evaded the detection of antivirus engines on VirusTotal almost entirely.

Reusing code from other malware is what helped this ransomware keep a low profile and not trigger antivirus alerts all this time. Details about its victims and the ransom demands are unknown at this time but now that it made it on researchers' radar, PureLocker will definitely get more attention from the infosec community.

Read More

Even More

More #News

- Zero Trust strategy—what good looks like
- GitHub launches 'Security Lab' to help secure open source ecosystem
- Two Charged Over Crypto Theft via SIM Swapping, Death Threats
- Telegram MTProxy Servers Used to DDoS Iranian Cloud Provider

- Mexico's Pemex Oil Suffers Ransomware Attack, $4.9 Million Demanded
- PCI DSS Compliance Between Audits is Declining: Verizon
- ASP.NET hosting provider recovering from ransomware attack
- New MITRE Foundation Aims to Boost Critical Infrastructure
- Alleged mastermind behind $20m stolen-card site extradited to US
- How to manage Siri privacy settings in iOS 13.2
- Visa Warns of New JavaScript Skimmer 'Pipka'
- Company Detected Years-Long Breach Only After Hacker Maxed Out Servers' Storage
- New ZombieLoad v2 Attack Affects Intel's Latest Cascade Lake CPUs
- Over 100,000 Fake Domains With Valid TLS Certificates Target Major Retailers

#Patch Time!

- Patch Tuesday, November 2019 Edition
- Microsoft Issues Guidance for Intel CPU Driver Security Flaws
- Intel Patched 77 Vulnerabilities in November 2019 Platform Update
- McAfee Patches Privilege Escalation Flaw in Antivirus Software
- Apple to fix Siri bug that exposed parts of encrypted emails
- Microsoft Releases the November 2019 Security Updates for Office
- Adobe squashes critical vulnerabilities in Illustrator CC, Media Encoder
- Qualcomm Bug Exposes Critical Data on Samsung, LG Phones
- DLL Hijacking Flaw Impacts Symantec Endpoint Protection
- Microsoft issues patch for Internet Explorer zero-day

#Tech and #Tools

- JWT Attack playbook with jwt_tool
- TFSec: Static analysis powered security scanner for your terraform code
- Bypass MS Defender on-diskwrite detection by renaming your malware
- Introducing iVerify, the security toolkit for iPhone users
- CVE-2019-1405 and CVE-2019-1322 – Elevation to SYSTEM via the UPnP Device Host Service and the Update Orchestrator Service
- Hunting for LoLBins
- Ghost Potato: NTLM Reflection Attack
- Keylogging users via Slack themes
- How Not to Implement reCAPTCHA
- GoQuery: Provide a shell like interface by utilizing osquery's distributed API
- Using Kibana and Packetbeat to map DNS queries
- RdpThief: Extracting Clear-text Credentials from Remote Desktop Clients
- Detecting Manual AWS Console Actions
- Beginner Network Pentesting course
- Automate the Creation of ATT&CK Navigator Group Layer Files with Python
- SCShell: Fileless lateral movement tool that relies on ChangeServiceConfigA to run command

Kingred Group is growing, so does the Group Security team! We're looking for new talented professionals to come join us. 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 a diverse team of 1,600 people serving over 26 million customers across Europe, Australia and the US. 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 is an innovation driven company that builds on trust.

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