Security Newsletter

20 May 2019

Subscribe to this newsletter

Cybersecurity's Week From Hell

Two years after WannaCry ransomware was unleashed, the cybersecurity realm isn't any calmer. This week, multiple flaws - all serious, all exploitable and some already being actively exploited in the wild - have come to light. Big names - including Cisco, Facebook, Intel and Microsoft - build the software and hardware at risk. And fixes for some of the flaws are not yet available.

A buffer overflow flaw in WhatsApp has been used to target individuals and apparently to install Pegasys spyware, built by Israel's NSO Group and sold to governments and law enforcement agencies.

Side-channel speculative execution flaws continue to be discovered in CPUs. This week, a team of researchers as well as Intel confirmed that they'd found more flaws in processors along the lines of the Spectre and Meltdown flaws that came to light in early 2018. Dubbed ZombieLoad, the vulnerabilities would allow an attacker to retrieve private data from a processor's buffers.

To block another WannaCry-type worm, Microsoft is urging many users to update Remote Desktop Services - formerly known as Terminal Services - to fix CVE-2019-0708 (see: To Prevent Another WannaCry, Microsoft Patches Old OSs).

Thangrycat: Research published this week shows that secure boot functionality built into many Cisco devices isn't secure.

Hence organizations will have to patch. But in the meantime, in some cases they're still waiting for patch release dates, and thus having to track when they might be able to start testing and then planning to roll out future fixes.

Read More BankInfoSecurity

Bluetooth Flaw Found in Google Titan Security Keys; Get Free Replacement

A team of security researchers at Microsoft discovered a potentially serious vulnerability in the Bluetooth-supported version of Google's Titan Security Keys that could not be patched with a software update. However, users do not need to worry as Google has announced to offer a free replacement for the affected Titan Security Key dongles.

In a security advisory published Wednesday, Google said a "misconfiguration in the Titan Security Keys Bluetooth pairing protocols" could allow an attacker who is physically close to your Security Key (~within 30 feet) to communicate with it or the device to which your key is paired. Launched by Google in August last year, Titan Security Key is a tiny low-cost USB device that offers hardware-based two-factor authentication (2FA) for online accounts with the highest level of protection against phishing attacks.

Microsoft originally discovered the vulnerability and disclosed it to Google, as well as Feitian, the company that makes Titan Keys for Google and also sells the same product (ePass) under its own brand. Feitian also made a coordinated disclosure about this vulnerability the same day as Google and is offering a free replacement program for its users. Google also says that the Bluetooth security key is still more secure than turning it off altogether or relying on other two-factor authentication methods like SMS or phone call.

Read More on TheHackerNews

Replacement programme for Feitian Keys

More #News

- Report Reveals TeamViewer Was Breached By Chinese Hackers In 2016

- Fxmsp Chat Logs Reveal the Hacked Antivirus Vendors, AVs Respond
- U.S. Govt Issues Microsoft Office 365 Security Best Practices
- Equifax's Data Breach Costs Hit $1.4 Billion
- Hackers Inject Magecart Card Skimmer in Forbes' Subscription Site
- Credential Stuffing attack on Uniqlo Exposes 460,000 Customer Accounts
- Google Payment Privacy Settings Hidden Behind Special URL
- GDPR: Europe Counts 65,000 Data Breach Notifications So Far
- Stack Overflow hacker went undetected for a week
- Microsoft Tech Support Scams Invade Azure Cloud Services
- Over 12,000 MongoDB Databases Deleted by Unistellar Attackers
- Intel MDS Vulnerabilities: What You Need to Know
- Google Starts Tracking Zero-Days Exploited in the Wild

#Patch Time!

- List of MDS Speculative Execution Vulnerability Advisories & Updates
- Microsoft's May 2019 Patch Tuesday Fixes 79 Vulnerabilities
- Linux Kernel Prior to 5.0.8 Vulnerable to Remote Code Execution in RDS
- Thangrycat Flaw Affecting Millions of Cisco Devices Let Attackers Implant Persistent Backdoor
- NVIDIA Patches High Severity Bugs in GPU Display Driver
- SAP Patches Multiple Missing Authorization Checks
- Update iOS and Mojave now! Apple patches are out
- Adobe security update released for critical Flash, Acrobat, Reader bugs
- Microsoft Releases May 2019 Office Updates With Security Fixes
- WhatsApp flaw lets hackers install spyware on iOS & Android devices
- Attackers Exploit WhatsApp Flaw to Auto-Install Spyware
- Remote Code Execution Vulnerability Impacts SQLite
- Linksys Smart Wi-Fi Routers Leak Info of Connected Devices
- Cisco Patches Critical Vulnerabilities in Prime Infrastructure (PI) Software
- Bug in WordPress Live Chat Plugin Lets Hackers Inject Scripts
- Faulty database script brings Salesforce to its knees
- Privilege Escalation Flaws Impact Wacom Update Helper
- Slack Flaw Allows Hackers to Steal, Manipulate Downloads
- Google recalls Titan Bluetooth keys after finding security flaw
- SSL/TLS fingerprint tampering jumps from thousands to billions
- Microsoft Patches 'Wormable' Flaw in Windows XP, 7 and Windows 2003

#Tech and #Tools

- Trivy: A Simple and Comprehensive Vulnerability Scanner for Containers, Suitable for CI
- 0day "In the Wild"
- Microsoft Releases Attack Surface Analyzer 2.0
- Stealing Downloads from Slack Users
- Pown CDB: a Chrome Debug Protocol utility

- CA/Certinomis Issues
- Exfiltration series: Certexfil
- Thrangrycat
- The NSO WhatsApp Vulnerability – This is How It Happened
- Frida 12.5 Released
- RIDL, FALLOUT and ZombieLoad
- Slicing onions: Part 1 – Myth-busting Tor.
- LES: Linux privilege escalation auditing tool
- Nuages: A modular C2 framework
- Combolist Generator

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 Security analyst position
- Interested in Governance, Risk and Compliance? Apply for our Information Security Specialist role

Kindred is one of the largest online gambling companies in the world with over 24 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 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