Security Newsletter

14 September 2020

Subscribe to this newsletter

New Unpatched Bluetooth Flaw Lets Hackers Easily Target Nearby Devices

Bluetooth SIG—an organization that oversees the development of Bluetooth standards—today issued a statement informing users and vendors of a newly reported unpatched vulnerability that potentially affects hundreds of millions of devices worldwide.

Dubbed 'BLURtooth' and tracked as CVE-2020-15802, the flaw exposes devices powered with Bluetooth 4.0 or 5.0 technology, allowing attackers to unauthorizedly connect to a targeted nearby device by overwriting the authenticated key or reducing the encryption key strength. In other words, the flaw leverage ability under specific implementations of the pairing process that could allow devices to overwrite authorization keys when the transport enforces a higher level of security.

"This may permit a Man In The Middle (MITM) attack between devices previously bonded using authenticated pairing when those peer devices are both vulnerable. The Bluetooth SIG further recommends that devices restrict when they are pairable on either transport to times when user interaction places the device into a pairable mode or when the device has no bonds or existing connections to a paired device," the researchers said.

Read More on TheHackersNews

Even More on BleepingComputer

Data center giant Equinix discloses ransomware incident

Equinix, one of the world's largest providers of on-demand colocation data centers, has disclosed today a security breach.Equinix says ransomware hit internal systems but that data centers are OK.

Equinix is just the latest in a long list of ransomware incidents that have impacted web hosting and data center providers. The list also includes CyrusOne, Cognizant, A2 Hosting, SmarterASP.NET, Dataresolution.net, and Internet Nayana. Such companies are ripe targets for cyber-criminals, and especially for ransomware gangs. The reasons are simple and involve the immediate effect of their attacks, which often bring down services for impacted companies, but also for their respective customers, all of whom are expecting near-perfect uptime.

There is no suggestion that the company is downplaying the incident, with no major outages being reported at the time of writing, and no wave of customer complaints flooding social media.

Read More on ZDNet

More #News

- Why Companies Need CISOs and CIOs as Board Members
- US Election Hack Attacks Traced to Russia, China, Iran
- Portland passes the strictest facial recognition technology ban in the US yet
- Raccoon attack allows hackers to break TLS encryption 'under certain conditions'
- Microsoft: State-backed hackers are targeting the 2020 US elections
- Hackers Stole $5.4 Million From Eterbase Cryptocurrency Exchange
- Money from bank hacks rarely gets laundered through cryptocurrencies
- Chilean bank shuts down all branches following ransomware attack

#Patch Time!

- Microsoft Patch Tuesday, Sept. 2020 Edition
- Microsoft Office September security updates fix critical RCE bugs
- Adobe Experience Manager, InDesign, Framemaker receive fixes for critical bugs in new update
- Vulnerabilities in CodeMeter Licensing Product Expose ICS to Remote Attacks
- Intel fixes critical flaw in corporate remote management platform
- Android's September 2020 Patches Fix Critical System Vulnerabilities
- Critical Access Control Vulnerability Patched in SAP Marketing
- Samsung fixes critical Android flaws with September updates
- Hackers are fighting a war over 300K vulnerable WordPress sites
- Palo Alto Networks Patches 6 Firewall Vulnerabilities
- Microsoft, Oracle, and Google top list of companies with most vulnerabilities disclosed in Q2

#Tech and #Tools

- Building a Secure Amazon S3 Bucket (AWS)
- Azure can now install security updates on Windows VMs automatically
- Security Controls in Azure Security Center: Enable Endpoint Protection
- WasmBoxC: Simple, Easy, and Fast VM-less Sandboxing
- OSINT Certificate Transparency Search
- Raccoon Attack
- Evading Censorship from the Server-side
- Security by Obscurity is Underrated
- Abusing dynamic groups in Azure AD for privilege escalation
- Security Group (SG) and Network Access Control List (NACL) configurations for Elastic Kubernetes Service (EKS)
- TREVORspray - O365 password sprayer
- What Happens When you Type Your Password into Windows?
- Introducing Red Commander: A Guidepoint Security Open Source Project

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