Talk Nerdy To Me

1

September 2022

Tesla Owner Implants Chip In Hand To Unlock, Start Car

A Michigan man never again has to worry about losing his car keys after he had a chip implanted in his hand that unlocks and starts his Tesla.

Brandon Dalaly had the chip implanted under local anesthetic at a tattoo and piercing parlor. A few days later, his hand hardly sore, he could use it to open his Tesla by hovering over the door pillar.

“You can’t lose your hand, so you always have a way of getting in your car,” Dalaly said.

Though he’s been mocked online as an Elon Musk groupie, Dalaly says he’s actually just a huge technology nerd. What he really wants is for the chip to be updated, so the implant will work for credit cards.

Until that’s possible, Dalaly will settle for using it to start his Tesla by holding his hand over the console.

“Getting a lot of comments saying, ‘What if someone comes after you and chops off your hand?’” Dalaly said.

He already has a chip implanted in his other hand that allows him to unlock the door to his home. It also holds his contact and medical information, such as COVID vaccinations. It glows green, so you know the phone is reading it.

Source: https://www.wpta21.com/

A High Severity TikTok Vulnerability Allowed One-click Account Hijacking

A vulnerability in the TikTok app for Android could have let attackers take over any account that clicked on a malicious link, potentially affecting hundreds of millions of users of the platform.

Details of the one-click exploit were revealed in a blog post from researchers on Microsoft's 365 Defender Research Team. The vulnerability was disclosed to TikTok by Microsoft, and has since been patched.

The bug and its resulting attack, labeled a "high severity vulnerability," could have been used to hijack the account of any TikTok user on Android without their knowledge, once they clicked on a specially crafted link. After the link was clicked, the attacker would have access to all primary functions of the account, including the ability to upload and post videos, send messages to other users, and view private videos stored in the account.

The potential impact was huge, as it affected all global variants of the Android TikTok app, which has a total of more than 1.5 billion downloads on the Google Play Store. However, there's no evidence it was exploited by bad actors.

"Through our partnership with security researchers at Microsoft, we discovered and quickly fixed a vulnerability in some older versions of the Android app," TikTok spokesperson Maureen Shanahan. "We appreciate the Microsoft researchers for their efforts to help identify potential issues so we can resolve them."

Microsoft confirmed that TikTok responded promptly to the report. "We gave them information about the vulnerability and collaborated to help fix this issue" Tanmay Ganacharya, partner director for security research at Microsoft Defender for Endpoint, told The Verge. "TikTok responded quickly, and we commend the efficient and professional resolution from the security team."

According to details published in the blog post, the vulnerability affected the deep link functionality of the Android app. This deep link handling tells the operating system to let certain apps process links in a specific way, such as opening the Twitter app to follow a user after clicking an HTML "Follow this account" button embedded in a webpage.

This link handling also includes a verification process that should restrict the actions performed when an application loads a given link. But the researchers found a way to bypass this verification process and execute a number of potentially weaponizable functions within the app.

One of these functions let them retrieve an authentication token tied to a certain user account, effectively granting account access without the need to enter a password. In a proof-of-concept attack, the researchers crafted a malicious link that, when clicked, changed a TikTok account's bio to read "SECURITY BREACH."

Fortunately, the vulnerability was detected, and Microsoft has used the opportunity to stress the importance of collaboration and coordination between technology platforms and vendors.

"As threats across platforms continue to grow in numbers and sophistication, vulnerability disclosures, coordinated response, and other forms of threat intelligence sharing are needed to help secure users' computing experience, regardless of the platform or device in use," wrote Microsoft's Dimitrios Valsamaras in the blog post. "We will continue to work with the larger security community to share research and intelligence about threats in the effort to build better protection for all."

Although the TikTok app is not known to have suffered any major hacks so far, some critics have branded it a security risk for other reasons.

Recently, concerns have been raised over the extent to which US users' data can be accessed by China-based engineers at ByteDance, TikTok's parent company. In July, Senate Intelligence Committee leaders called on FTC chair Lina Khan to investigate TikTok after reports brought into question claims that US users' data was walled off from the Chinese branch of the company.

Source: https://www.theverge.com/

Our CEO Is A Published Author

Stay one step ahead of cyber criminals to protect your business, your customers, and your money!

In Jason's first published book, he talks about why cybercrime today cannot be ignored and why your network and data are cyber criminals' #1 target!

Learn all the ways to protect yourself and your data. Contact us today for your copy of *Inside The Hacker Mind.*

This Month In History

September 4, 1998 - Google filed for official incorporation.

September 3,1995 - eBay was founded and the first item sold was a broken laser pointer.

September 4, 1956 - The first commercial hard drive was announced. It held about 4 to 5 MB.

September 1, 1977 - Pioneer 11 is the first man-made object to fly by Saturn.

September 2022

Grabbing The Bull By The Hornes - Preferred IT CEO, Jason Horne, Is Gaining Ground Fast

Check out Preferred IT Group's CEO, Jason Horne in MSP Success Magazine!

"So, in the sports bar that night, where patrons sampled cold beer and cheered on the Cubs and Komets, a vision for what would become Preferred IT emerged."

FUN FACT!

preferred group IT

CONTACT US

Fort Wayne
260.440.7377

Warsaw
574.306.4288

Columbia City
260.213.4266

Indianapolis
317.426.8180

www.preferreditgroup.com

6333 Constitution Drive
Fort Wayne, IN 46804

Subscribe to our blog and follow us on social media.