Medieninformation

TECHNISCHE UNIVERSITÄT DARMSTADT

Wenn das iPhone schwarz wird

Massive Sicherheitslücke im mobilen Betriebssystem von Apple

Darmstadt, 31. Oktober 2018. Ein Forschungsteam der TU Darmstadt hat eine Schwachstelle in Apples iOS gefunden, die mehr als eine halbe Milliarde Geräte betrifft. Die Forscher empfehlen Nutzern dringend, das soeben erschienene Update 12.1 zu installieren. Aufgrund der Sicherheitslücke können Angreifer iPhones und iPads mit handelsüblicher Hardware und ohne physischen Zugriff zum Abstürzen bringen.

Kommunikation und Medien
Corporate Communications

Karolinenplatz 5
64289 Darmstadt

Ihr Ansprechpartner:
Jörg Feuck
Tel. +49 6151 16 - 20018
feuck@pvw.tu-darmstadt.de
www.tu-darmstadt.de/presse
presse@tu-darmstadt.de

Wissenschaftler des Secure Mobile Networking Labs an der TU Darmstadt haben eine Schwachstelle im iPhone-Betriebssystem iOS 12 gefunden, durch die ein Angreifer mobile Apple-Geräte wie iPhones und iPads mit einer Standard-WLAN-Karte und einer für unter 20 Euro erhältlichen programmierbaren Platine zum Absturz bringen kann. Nach dem Prinzip der „responsible disclosure“ wurde die Sicherheitslücke an Apple gemeldet und soeben durch ein iOS-Update geschlossen. Die Wissenschaftler empfehlen Nutzern von mobilen Geräten von Apple dringend, das aktuelle iOS-Update 12.1 zu installieren, um die Geräte zu schützen.

Apple wirbt traditionell für nutzerfreundliche Funktionen, wie beispielsweise AirPlay, mit dem man kabellos und mit einem Klick von verschiedensten Apple-Geräten Musik oder Filme an kompatible Lautsprecher und Fernseher senden kann. Die dahinterliegenden Protokolle nutzen dazu Herstellererweiterungen wie Apple Wireless Direct Link (AWDL), welches direkte WLAN-Kommunikation zwischen Apple-Geräten ermöglicht. Doch die komfortablen Funktionen bergen auch Risiken, erklärt TU-Professor Matthias Hollick, Leiter des Secure Mobile Networking Labs: „AWDL nutzt verschiedene Funktechnologien. Vereinfacht gesagt klingeln wir mittels Bluetooth LE Sturm und das Zielgerät aktiviert dadurch AWDL. In einem zweiten Schritt nutzen wir aus, dass Apple die Eingaben, die wir an das Zielgerät schicken, nicht vollständig sauber überprüft; das ermöglicht es uns, das Gerät mit unsinnigen Eingaben zu fluten. Im Ergebnis können wir dadurch das Zielgerät oder auch alle in der Nähe befindlichen Geräte gleichzeitig zum Absturz bringen. Dabei benötigen wir keinerlei Nutzerinteraktion.“

Milan Stute, Mitarbeiter am Secure Mobile Networking Lab, ergänzt: „Um die Bluetooth Brute-Force-Attacke und die nachfolgenden Schritte praktisch durchzuführen, braucht es nicht einmal spezielle Hardware: der

Angriff funktioniert mit einer WLAN-Karte eines handelsüblichen Laptops und einem BBC micro:bit, einem preiswerten Bluetooth-fähigen Einplatinencomputer ähnlich einem Raspberry Pi oder Arduino, der ursprünglich als Programmier-Lernplattform für Schulkinder entwickelt wurde.“ Potenzielle Angreifer hätten also leichtes Spiel. Das demonstrieren die Forscher in einem Video des – nach erfolgreich installiertem Update so nicht mehr möglichen – Angriffs, das sie auf YouTube (https://www.youtube.com/watch?v=M5D9NeKapUo) veröffentlicht haben. Reihenweise stürzen die Geräte ab, ohne dass die Forscher sie dafür auch nur einmal berühren mussten.

Um die Schwachstelle – veröffentlicht als CVE-2018-4368 – überhaupt entdecken zu können, mussten die Forscher das proprietäre AWDL-Protokoll zunächst verstehen und in einem eigenen Prototypen nachbauen. Mit diesem wurde es dann möglich, die Schwachstelle auszunutzen.

Auch wenn die gefundene Schwachstelle nur Apple-Geräte betrifft, sollten sich Nutzer mit einem Android-Handy nicht in Sicherheit wiegen: Die gefundene Schwachstelle hat auch Implikationen für die „Nicht-Apple-Welt“. Der neue Standard der Wi-Fi Alliance, Neighbor Awareness Networking (NAN), baut auf AWDL auf und wird bereits von Googles Android unterstützt (https://www.wi-fi.org/discover-wi-fi/wi-fi-aware). Die Forscher erwarten, dass ähnliche Schwachstellen in NAN-Implementierungen gefunden werden, da AWDL und NAN eine ähnlich hohe Komplexität aufweisen.

Wissenschaftliche Veröffentlichung
M. Stute, D. Kreitschmann, and M. Hollick, “One Billion Apples’ Secret Sauce: Recipe for the Apple Wireless Direct Link Ad hoc Protocol,” In: The 24th Annual International Conference on Mobile Computing and Networking (MobiCom ’18), 2018.
Link zur Publikation: https://owlink.org

iOS 12.1 Release Notes: https://support.apple.com/kb/HT201222

CVE: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4368

Die TU Darmstadt zählt zu den führenden Technischen Universitäten in Deutschland. Sie verbindet vielfältige Wissenschaftskulturen zu einem charakteristischen Profil. Ingenieur- und Naturwissenschaften bilden den Schwerpunkt und kooperieren eng mit prägnanten Geistes- und

TECHNISCHE UNIVERSITÄT DARMSTADT

Sozialwissenschaften. Weltweit stehen wir für herausragende Forschung in unseren hoch relevanten und fokussierten Profilbereichen: Cybersecurity, Internet und Digitalisierung, Kernphysik, Energiesysteme, Strömungsdynamik und Wärme- und Stofftransport, Neue Materialien für Produktinnovationen. Wir entwickeln unser Portfolio in Forschung und Lehre, Innovation und Transfer dynamisch, um der Gesellschaft kontinuierlich wichtige Zukunftschancen zu eröffnen. Daran arbeiten unsere 312 Professorinnen und Professoren, 4.450 wissenschaftlichen und administrativ-technischen Mitarbeiterinnen und Mitarbeiter sowie knapp 26.000 Studierenden. Mit der Goethe-Universität Frankfurt und der Johannes Gutenberg-Universität Mainz bildet die TU Darmstadt die strategische Allianz der Rhein-Main-Universitäten.

MI-Nr. 57/2018, akbr/feu