Medieninformation

TECHNISCHE UNIVERSITÄT DARMSTADT

Da ist der Wurm drin

Apple-Geräte erlauben Datenklau und stürzen ab

Kommunikation und Medien
Corporate Communications

Karolinenplatz 5
64289 Darmstadt

Ihr Ansprechpartner:
Jörg Feuck
Tel. 06151 16 - 20018
Fax 06151 16 - 23750
feuck@pvw.tu-darmstadt.de

www.tu-darmstadt.de/presse
presse@tu-darmstadt.de

Darmstadt, 16. Mai 2019. Ein internationales Forscherteam unter Beteiligung der TU Darmstadt hat Sicherheits- und Privatheitsprobleme in iOS und macOS entdeckt. Apple hat mittlerweile Updates zur Behebung veröffentlicht.

Jessica will mit ihrem iPhone zu ihrem Flug nach New York einchecken, doch der Bildschirm bleibt schwarz, während das Telefon ständig neu startet. Und sie ist damit nicht alleine: Alle Nutzer von Apple-Geräten in der Nähe haben dasselbe Problem. Was sie nicht weiß: Als sie in der Flughafenlounge Fotos und Firmenpräsentationen von ihrem Handy zu ihrem MacBook übertragen hat, konnte ein Angreifer diese mitlesen, ihren Standort nachverfolgen und diesen sogar mit ihrem Vornamen und einer Geräte-ID assoziieren.

Diese Schwachstellen wurden von Forschern der TU Darmstadt und der Northeastern University Boston entdeckt. Gemeinsam mit dem Apple-Sicherheitsteam arbeiteten die Forscher an der Behebung der Lücken. Sie empfehlen Nutzern von Apple-Geräten dringend, die soeben veröffentlichten Updates iOS 12.3 und macOS 10.14.5 zu installieren, um die Sicherheitsverbesserungen zu erhalten.

Mehr als eine Milliarde Apple-Geräte waren prinzipiell von den Schwachstellen betroffen, da diese in einem gemeinsamen Kernbestandteil aller Apple-Betriebssysteme wie iOS und macOS verborgen waren: ein proprietäres Protokoll namens Apple Wireless Direct Link (AWDL), über das bisher nicht viel bekannt war. Zahlreiche Sicherheits- und Privatheitsprobleme darin ermöglichten es einem Angreifer, Handynutzer zu orten, ihre Geräte abstürzen zu lassen, Kommunikation zu unterbinden und sensible Daten bei der Übermittlung per AirDrop abzufangen.

AWDL macht es möglich Nutzer zu verfolgen, da es die ID und den Gerätenamen preisgibt, der in vielen Fällen den Vornamen des Besitzers enthält. Milan Stute, Forscher an der TU Darmstadt und im Nationalen Forschungszentrum für angewandte Cybersicherheit CRISP, erklärt: „Wir erforschen die Drahtlos-Funktionen von Apple seit 2017, um zu verstehen wie AWDL und die damit zusammenhängenden Dienste funktionieren. Zusätzlich zu den bereits erwähnten Privatheitsproblemen haben wir so auch einige Sicherheitsschwachstellen aufgedeckt.“ Das Forscherteam fand heraus, wie per AirDrop übertragene Dateien abgefangen werden können.

AirDrop ist ein Apple-Dienst, der auf AWDL aufbaut. Der potentielle Angreifer nutzt aus, dass die Benutzeroberfläche auch nicht vertrauenswürdige Verbindungen anzeigt. Mit einer solchen kann er eine sogenannte „man-in-the-middle“-Position erlangen und dadurch Dateien während der Übertragung abfangen oder modifizieren. Die Forscher haben ein Video auf YouTube veröffentlicht, das den Angriff demonstriert (https://youtu.be/5T7Qatoh0Vo).

Um überhaupt an AWDL und AirDrop forschen zu können, mussten die Wissenschaftler die Protokolle zuerst rekonstruieren und selbst implementieren. Ihre Versionen haben sie als Open Source Software veröffentlicht, um sie anderen Forschern zugänglich zu machen (https://owlink.org). Die zugehörige wissenschaftliche Veröffentlichung wird im August auf dem renommierten USENIX Security Symposium 2019 präsentiert.

Professor Matthias Hollick, Forschungsgruppenleiter an der TU Darmstadt und am Nationalen Forschungszentrum für angewandte Cybersicherheit CRISP, fasst die Problematik zusammen: „Apple ist eines der wenigen großen Technologie-Unternehmen, das die Sicherheit und Privatheit seiner Nutzer und die einfache Bedienbarkeit seiner Produkte in den Mittelpunkt stellt. Es wäre schön, wenn sich andere Tech-Riesen dem anschließen würden. Deswegen ist es nahezu ironisch, dass Apple der komplexe Aufbau eines seiner wichtigsten Drahtlosprotokolle zum Verhängnis wurde, das als Basis für die benutzerfreundlichen Features des Apple-Kosmos dient. In diesem Fall ging der Wunsch nach größtmöglicher Funktionalität zu Lasten der Sicherheit. Es wäre viel geholfen, wenn Hersteller sich auf einfache und offene Lösungen fokussieren.“

Wissenschaftliche Veröffentlichung zum Thema

Milan Stute, Sashank Narain, Alex Mariotto, Alexander Heinrich, David Kreitschmann, Guevara Noubir, and Matthias Hollick. "A Billion Open Interfaces for Eve and Mallory: MitM, DoS, and Tracking Attacks on iOS and macOS Through Apple Wireless Direct Link" in USENIX Security '19.
https://www.usenix.org/conference/usenixsecurity19/presentation/stute

Hintergrund CRISP

Die Wissenschaftsstadt Darmstadt ist mit der TU Darmstadt und dem Nationalen Forschungszentrum für angewandte Cybersicherheit CRISP einer der wichtigsten Forschungsstandorte für Cybersicherheit weltweit. In CRISP forschen und entwickeln über 450 Wissenschaftlerinnen und Wissenschaftler an wichtigen Problemen und Fragen zum unmittelbaren Nutzen von Gesellschaft, Wirtschaft und Staat.

CRISP ist eine Einrichtung der Fraunhofer-Gesellschaft für ihre beiden Darmstädter Institute SIT und IGD unter Beteiligung der Technischen Universität Darmstadt und der Hochschule Darmstadt. Es wird gefördert vom Bundesministerium für Bildung und Forschung (BMBF) und vom Hessischen Ministerium für Wissenschaft und Kunst (HMWK).

Über die TU Darmstadt

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 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.
www.tu-darmstadt.de

MI-Nr. 33/2019, akbr