NACHRICHTEN AG

31. Juli 2024

Sicherheitslücken beim WLAN-Calling: Forschung aus Saarbrücken schlägt Alarm

Eine Sicherheitslücke beim WLAN-Calling betrifft Millionen Nutzer weltweit. Forscher aus Saarbrücken warnen vor möglichen Abhöraktionen. Erfahren Sie mehr!

WLAN-Calling und die Auswirkungen einer Sicherheitslücke

Stand: 31.07.2024 15:43 Uhr

Eine kürzlich entdeckte Sicherheitslücke bei WLAN-Calling könnte Millionen von Nutzern sowie Netzbetreibern weltweit schwerwiegende Probleme bereiten. Die von Forscher Adrian Dabrowski und seinem Team vom Cispa Helmholtz-Zentrum für Informationssicherheit in Saarbrücken identifizierte Schwachstelle betrifft insbesondere Nutzer in mehreren Ländern, darunter Österreich, die Slowakei, Brasilien und Russland.

Was ist WLAN-Calling?

WLAN-Calling, auch bekannt als Voice over WiFi (VoWiFi), ermöglicht es modernen Smartphones, Telefonanrufe über ein WLAN-Netzwerk statt über das Mobilfunknetz herzustellen. Dies ist besonders nützlich an Orten mit schwachem Mobilfunkempfang, wie in Tunneln oder Untergeschossen. Die Einführung dieser Technologie erfolgte bereits im Jahr 2016.

Details zur Sicherheitslücke

Die Forscher fanden heraus, dass es bei 13 von 275 untersuchten Mobilfunkanbietern erhebliche Sicherheitsmängel gab, die die Kommunikation von rund 140 Millionen Kunden gefährdeten. Laut Dabrowski war eine unzureichende Verschlüsselung der Grund für diese Sicherheitslücke. Dadurch konnten potenziell Smartphone-Hersteller sowie Sicherheitsbehörden in den betroffenen Ländern auf die Kommunikation zugreifen.

Betroffene Geräte und Hersteller

Ein weiterer Aspekt der Sicherheitslücke betrifft bestimmte Chips des taiwanesischen Herstellers MediaTek, die in zahlreichen Android-Smartphones, unter anderem von Xiaomi, Oppo, Realme und Vivo, verbaut sind. Angreifer hätten laut den Forschern in der Lage sein können, die Verschlüsselung der Smartphones auf eine schwächere Stufe zu reduzieren, was das Abhören erleichtert hätte.

Reaktionen und Maßnahmen

Obwohl es unklar bleibt, wie viele Nutzer weltweit tatsächlich von einem Abhörangriff betroffen waren, haben die Hersteller bereits Updates bereitgestellt, die die aufgezeigten Sicherheitslücken schließen sollen. Diese schnellen Reaktionen sind entscheidend, um das Vertrauen der Nutzer in die Technologie aufrechtzuerhalten und mögliche Datenschutzverletzungen zu minimieren.

Fazit

Die Entdeckung dieser Sicherheitslücke verdeutlicht die Bedeutung von fortlaufenden Sicherheitsüberprüfungen in der Technologiebranche. Nutzer und Anbieter müssen wachsam bleiben, um die Sicherheit ihrer Kommunikation zu

gewährleisten. Das Cispa und andere Forschungsinstitute spielen eine zentrale Rolle, um kritische Sicherheitsfragen zu identifizieren und zu adressieren.

– **NAG**

Details

Besuchen Sie uns auf: n-ag.de