Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

FragAttacks - Neue WLAN-Schwachstellen

Nachezu alle WLAN-Geräte betroffen

CSW-Nr. 2021-216748-1132, Version 1.1, 14.05.2021

IT-Bedrohungslage*: 3 / Orange

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

TLP:WHITE: Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE ohne Einschränkungen frei weitergegeben werden.

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP finden Sie am Ende dieses Dokumentes.

Sachverhalt

Unter der Bezeichnung "FragAttacks" (fragmentation and aggregation attacks) veröffentlichten Sicherheitsforscher am Dienstag, den 11. Mai 2021, Erkenntnisse zu zahlreichen WLAN-Schwachstellen, die sowohl WLAN-Router als auch die damit verbundenen Geräte betreffen können [FRA2021a]. Nach derzeitiger Sachlage ist davon auszugehen, dass einige der Sicherheitslücken designbedingt im Wi-Fi-Standard vorliegen und somit herstellerübergreifend ausgenutzt werden können. Die verwendete Verschlüsselungstechnik spielt für Attacken ebenfalls keine Rolle. Ferner führen die Sicherheitsforscher aus, dass jedes von ihnen getestete WLAN-Gerät von mindestens einer der genannten Schwachstellen betroffen ist. Eine detaillierte Beschreibung der Sicherheitslücken und Bedrohungsszenarien kann unter [FRA2021a] eingesehen werden.

Vorab durch die Entdecker informierte Hersteller haben die Möglichkeit erhalten, den Sachverhalt zu prüfen und ggf. Patches bereitzustellen. ~~Aktuell liegen dem BSI keine Informationen vor, welche Geräte von welchen Schwachstellen betroffen sind bzw. ob Patches veröffentlicht wurden/werden.~~

Update 1:
Eine Liste betroffener Hersteller und verfügbarer Updates finden sich in der Kurzinfo CB-K21/0519 [BSI2021a].

* 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau.
2 / Gelb IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs.
3 / Orange Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs.
4 / Rot Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden.

Bewertung

Zum aktuellen Zeitpunkt ist davon auszugehen, dass nur eine lokale Ausnutzung der Schwachstellen möglich ist – also dann, wenn sich ein Angreifer in Reichweite eines Access Points oder Endgeräts eines potenziellen Opfers befindet. Gleichzeitig stellt die mögliche Betroffenheit zahlreicher – ggf. sogar aller – WLAN-Geräte ein erhebliches Risiko für Betreiber und Nutzer dar.

Je nach Schadenspotenzial der Sicherheitslücken könnte ein Täter außerdem bei einem lokalen Angriff an Informationen gelangen, die ihm anschließend weitere Attacken im jeweiligen Netz bzw. ggf. auch aus der Ferne ermöglichen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) war in den Coordinated Vulnerability Disclosure-Prozess nicht eingebunden. Eine detaillierte Bewertung ist daher zum aktuellen Zeitpunkt nicht möglich.

Maßnahmen

Das BSI empfiehlt, umgehend Herstellerwebseiten entsprechend der eingesetzten WLAN-Komponenten auf Informationen zu diesem Sachverhalt zu prüfen und bereitgestellte Patches zeitnah zu installieren. Die Installation sollte unter Beachtung des Ergebnisses einer Risikoanalyse durchgeführt werden. Bislang ungepatchte Schwachstellen in den Geräten müssen im Zusammenhang mit diesem Sachverhalt neu bewertet werden, da sich durch die potenzielle Umgehung der Verschlüsselung ggf. eine geänderte Bedrohungslage und damit ein geändertes Risiko ergibt.

Sofern keine Updates zur Verfügung stehen, kann die Gefahr der Ausnutzung einiger Sicherheitslücken durch die Verwendung von HTTPS reduziert werden. Einen umfassenden Schutz bietet diese Maßnahme jedoch selbstverständlich nicht.

Die Verwundbarkeit von WLAN-Geräten kann ggf. mithilfe des unter [FRA2021b] bereitgestellten Tools identifiziert werden. Weitere Informationen zum sicheren Betrieb von WLAN-Netzen stellt das BSI unter [BSI2021b] zur Verfügung.

Links

[FRA2021a] - FragAttacks: Security flaws in all Wi-Fi devices
https://www.fragattacks.com

[FRA2021b] - FragAttacks Tool
https://github.com/vanhoefm/fragattacks

[BSI2021a] - Kurzinfo CB-K21/0519 - IEEE 802.11 (WLAN): Mehrere Schwachstellen
https://cert-bund.de/advisoryshort/CB-K21-0519

[BSI2021b] - BSI - Bundesamt für Sicherheit in der Informationstechnik - NET.2.1: WLAN-Betrieb (Edition 2020)
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs/09_NET_Netze_und_Kommunikation/NET_2_1_WLAN_Betrieb_Edition_2020.pdf

Anlagen

Kontakt

Bitte wenden Sie sich bei allen Rückfragen zu diesem Dokument an denjenigen Kontakt, der Ihnen das Dokument zugesendet hat. Dadurch bleibt der Informationsfluss kanalisiert. Die Single Points of Contact (SPOCs) welche das Dokument direkt vom Nationalen IT-Lagezentrum des BSI erhalten haben, können sich direkt an die bekannten Kontaktdaten des Nationalen IT-Lagezentrums im BSI wenden.

Erklärungen zum Traffic Light Protokoll (TLP)

Dieses Dokument und die darin enthaltenen Informationen sind gemäß dem TLP eingestuft:

1) Was ist das Traffic Light Protokoll?

   Das TLP ist ein von der OECD entworfenes Protokoll, welches die Weitergabe von sensitiven Informationen innerhalb eines Informationsverbundes regelt. Die vom Autor adressierten Empfänger dieses Dokumentes haben sich im Vorfeld schriftlich verpflichtet das TLP zu beachten und das Dokument entsprechend den „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten.

2) Welche Einstufungen existieren?

   - **TLP:WHITE: Unbegrenzte Weitergabe**
     Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE ohne Einschränkungen frei weitergegeben werden.
   - **TLP:GREEN: Organisationsübergreifende Weitergabe**
     Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner frei weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden.
   - **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Verteilung**
     Informationen dieser Stufe darf der Empfänger innerhalb seiner Organisation auf Basis „Kenntnis nur wenn nötig“ weitergeben. Der Empfänger darf die Informationen zudem an Dritte weitergeben, soweit diese die Informationen zum Schutz des Empfängers oder zur Schadensreduktion beim Empfänger benötigen. Hierfür muss er sicherstellen, dass die „Dritten“ das TLP kennen und die damit verbundenen Regeln einhalten. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.
   - **TLP:RED: Persönlich, nur für benannte Empfänger**
     Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. Meistens werden TLP:RED-Informationen mündlich oder persönlich übergeben.

3) Was mache ich, wenn ich das Dokument an jemanden außerhalb des im TLP vorgegebenen Informationsverbundes weitergeben will?

   Sollte eine Weitergabe an einen nicht durch die Einstufung genehmigten Empfängerkreis notwendig werden, so ist diese vor einer eventuellen Weitergabe durch den Informationsersteller nachvollziehbar zu genehmigen. Bei ausnahmsweiser Weitergabe im Rahmen einer bestehenden gesetzlichen Verpflichtung ist der Informationsersteller – nach Möglichkeit vorab – zu informieren.

4) Was passiert, wenn ich die Einstufung nicht beachte?

   Bei Verstoß gegen die Regeln zur Weitergabe von Informationen erhält der Verpflichtete zukünftig nur noch TLP:WHITE eingestufte Informationen aus dem Kreis der Verpflichteten.