Digitaler Behördenfunk: Massive Schwachstellen bei TETRA entdeckt

Originalartikel

Backup

<html> <figure class=„aufmacherbild“><figcaption class=„akwa-caption“>(Bild: Daniel AJ Sokolov)</figcaption></figure> Der TETRA-Funkstandard wird vor allem von Behörden genutzt. Doch die international genutzte Verschlüsselung hat eine Hintertür. Gleich fünf Schwachstellen hat der Funkstandard TETRA (Terrestrial Trunked Radio). TETRA wurde in Europa entwickelt und wird weltweit vor allem für digitalen Behördenfunk genutzt [1]. Einrichtungen wie die Polizei, Militärs und Gefängnisverwaltungen legen großen Wert auf Verschlüsselung. Für sie sind die „Tetra:Burst“ genannten Schwachstellen eine üble Nachricht. Zumindest eine Lücke ist sogar absichtlich eingebaut, um die Verschlüsselung der Exportversion Tetras zu schwächen und die Kommunikation einfach abhörbar zu machen. Aufwändige Recherchen haben Carlo Meijer, Wouter Bokslag und Jos Wetzels von der niederländischen IT-Sicherheitsfirma Midnight Blue auf die Spur der fünf Schwachstellen gebracht. Tetra wurde 1995 vom Europäischen Institut für Telekommunikationsnormen (ETSI) standardisiert. Die Normungsinstitution ist prinzipiell dafür bekannt, die Wünsche von Sicherheitsbehörden nach „rechtmäßigem Zugang“ (Lawful Interception, LI) in internationale technische Standards [2] zu integrieren. <h3 class=„subheading“ id=„nav_geheimer0“>Geheimer Standard mit Hintertür</h3> Tetra ist das am weitesten verbreitete Funksystem der Polizei und anderer Blaulichtbehörden weltweit. Die Geräte stammen beispielsweise von Airbus, Damm, Hytera, Motorola oder Sepura. Der Funkstandard kommt in über 100 Ländern auf allen besiedelten Kontinenten zum Einsatz, nur in Nordamerika nutzen die Behörden vorrangig andere Funksysteme. Die nun ausgemachten Schwachstellen [3] blieben der breiten Öffentlichkeit jahrelang unbekannt, da ETSI die Verschlüsselungsalgorithmen geheim hielt. Der Standard umfasste zunächst mit TEA1 bis TEA4 vier einschlägige Programmroutinen zur Verschlüsselung, die von den Herstellern von Funkgeräten je nach Verwendungszweck und Kunde in verschiedenen Produkten verwendet werden können. TEA1 ist prinzipiell für kommerzielle Zwecke bestimmt, also etwa für Funkgeräte, die in kritischen Infrastrukturen (Kritis) in Europa und im Rest der Welt verwendet werden. Laut einem ETSI-

Dokument soll dieser Algorithmus auch für Geräte verwendet werden, die an Staaten mit autoritären Regimen wie den Iran gehen. Alle vier Tetra-Verschlüsselungsalgorithmen verwenden 80-Bit-Schlüssel, die auch mehr als zwei Jahrzehnte nach ihrer Veröffentlichung als nicht sonderlich leicht zu knacken gelten. Bei TEA1 stießen die Forscher nun aber auf eine Funktion, die den Schlüssel auf nur 32 Bit reduziert. Dem Team gelang es, diese Version mit einem Standard-Laptop und einer billigen Funk-Software in weniger als einer Minute zu brechen. Dabei handelt es sich offenbar um die Exportvariante für Länder, die der EU als nicht sonderlich freundlich gegenüberstehen. Der Einsatz von TEA2, wo die Experten die Hintertür nicht finden konnten, ist dagegen Polizei, Rettungsdiensten, Militär und Geheimdiensten in Europa vorbehalten. TEA3 wiederum ist für Staaten wie Mexiko oder Indien gedacht, die als „EU-freundlich“ gelten. TEA4 ist eine Alternative zu TEA1, wird aber so gut wie nicht genutzt. <h3 class=„subheading“ id=„nav_ag_kritis_gibt1“>AG Kritis gibt Entwarnung für Deutschland</h3> Für Deutschland haben Experten der AG Kritis teils Entwarnung gegeben [4]: TEA1 wird ihnen zufolge hierzulande allenfalls für die „Luftschnittstellenverschlüsselung ziviler Anwender“ eingesetzt. Die hiesigen Behörden und Organisationen mit Sicherheitsaufgaben (BOS) nutzten TEA2 und zusätzlich Ende-zu-Ende-Verschlüsselung [5]. Für betroffene Länder beschreibt das US-Magazin „Wired“ die Lage wenig rosig [6]: Dort hätten Angreifer die Kommunikation nicht nur abhören, sondern Befehle an Tetra-Funkgeräte senden können, um etwa Stromausfälle auszulösen. In den USA gehörten Energieversorger, eine Grenzschutzbehörde, eine Ölraffinerie, Chemiefabriken, ein großes Nahverkehrssystem an der Ostküste, drei internationale Flughäfen und eine Trainingsbasen der Armee zu den Nutzern. Eine der anderen Schwachstellen kann Angreifern ermöglichen, nicht nur Sprach- und Datenkommunikation zu entschlüsseln, sondern auch betrügerische Nachrichten zu versenden. Sie betrifft beispielsweise das niederländische TETRA-System C2000, das dort landesweit von Polizei, Feuerwehr und Rettung genutzt wird. Dabei wäre es möglich, Falschinformationen zu verbreiten oder Helfer und Streitkräfte umzuleiten. Die Forscher haben die Lücken schon 2021 gefunden und gemeldet. Sie stimmten dabei zu, ihre Erkenntnisse erst nach längerer Frist öffentlich zu machen. Das verschaffte Funkgeräteherstellern Zeit, Sicherheitsupdates und Abhilfemaßnahmen bereitzustellen. <h3 class=„subheading“ id=„nav_hintertür_von2“>Hintertür von Geheimdiensten ausgenutzt</h3> ETSI begrüßt laut einer Erklärung [7] „Forschungsbemühungen, die zur Stärkung von Standards beitragen“. Es seien „keine Schwächen in den TEA2- und TEA3-Algorithmen festgestellt“ worden. Tetra-Anbieter böten mittlerweile Updates sowie die Migration auf den neuen Algorithmensatz TEA5 bis TEA7 vom Oktober an. Diese Schritte verringerten auch das Potenzial, „die Identität von Mobilfunkendgeräten durch das Abfangen von Steuernachrichten von Basisstationen zu ermitteln“. Zudem könnten verschlüsselte Datenströme nicht mehr durch vorgetäuschte Basisstationen kompromittiert werden. Bei TEA1 helfe die gute alte Ende-zu-Ende-Verschlüsselung, übertragene Inhalte zu schützen, obwohl die

Verschlüsselung der Luftschnittstelle nun gebrochen ist. Eine ETSI-Sprecherin sagte dem US-Magazin „Motherboard“ [8]: „Die Tetra-Sicherheitsstandards wurden gemeinsam mit nationalen Sicherheitsbehörden festgelegt und sind für Exportkontrollbestimmungen konzipiert [9].“ Das Midnight-Blue-Team hat in den Snowden-Leaks Hinweise darauf gefunden, dass die NSA und ihr britisches Pendant GCHQ in der Vergangenheit TETRA in Malaysia und Argentinien abgehört haben. Bart Jacobs, Professor für Softwaresicherheit an der Universität Nijmegen, hofft, dass die Erkenntnisse „wirklich das Ende“ geschlossener, proprietärer Verschlüsselungslösungen bedeuten, „die nicht auf offenen, öffentlich geprüften Standards basieren“. Die Forscher wollen ihre Ergebnisse in den nächsten Monaten auf mehreren Konferenz präsentieren, darunter im August auf der Black Hat 2023 in Las Vegas sowie der Usenix Security in Anaheim und dem CCC Sommercamp in Berlin. () URL dieses Artikels:<small><code>https://www.heise.de/-9226620</code></small> Links in diesem Artikel:<small><code>[1] https://www.heise.de/news/Digitaler-Behoerdenfunk-Bund-beziffert-Milliarden-Ausgaben-1632175.html</code></small><small><code>[2] https://www.heise.de/tp/features/Die-ETSI-Dossiers-3448017.html</code></small><small><code>[3] https://www.midnightblue.nl/tetraburst</code></small><small><code>[4] https://twitter.com/honkhase/status/1683477305404866565</code></small><small><code>[5] https://www.heise.de/news/Digitaler-Behoerdenfunk-EADS-erfuellt-Kryptoanforderungen-198330.html</code></small><small><code>[6] https://www.wired.com/story/tetra-radio-encryption-backdoor/</code></small><small><code>[7] https://www.etsi.org/newsroom/news/2260-etsi-and-tcca-statement-to-tetra-security-algorithms-research-findings-publication-on-24-july-2023</code></small><small><code>[8] https://www.vice.com/en/article/4a3n3j/backdoor-in-police-radios-tetra-burst</code></small><small><code>[9] https://www.heise.de/tp/features/Update-Kryptopolitik-3411894.html</code></small><small><code>[10] mailto:ds@heise.de</code></small> Copyright © 2023 Heise Medien </html>