



SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

TETRA:BURST - Mehrere Schwachstellen in TEA-Algorithmen veröffentlicht

CSW-Nr. 2023-257705-1032, Version 1.0, 10.08.2023

IT-Bedrohungslage*: 2 / Gelb

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:CLEAR: Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten, die das TLP explizit nicht adressiert, dürfen Informationen der Stufe TLP:CLEAR 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

Am 24. Juli 2023 wurden 5 Schwachstellen in Terrestrial Trunked Radio Standard (TETRA) über Presseberichte öffentlich bekanntgegeben, die bereits 2021 von Midnight Blue entdeckt wurden. Die Forschenden stellten ihre Ergebnisse auf der Black Hat Konferenz am 9. August 2023 vor und veröffentlichten ihre Forschungsergebnisse [MNBL2023].

TETRA wurde 1995 vom European Telecommunications Standards Institute (ETSI) veröffentlicht und wird für eine abhörsichere Radio-Kommunikation von Regierungseinrichtungen, Rettungsdiensten und kommerziellen Organisationen genutzt. TETRA kann sowohl für Audio- als auch Datenübertragung verwendet werden. Zur Absicherung der Übertragung nutzt TETRA proprietäre kryptografische Algorithmen, die nur sehr wenigen Parteien unter einem Non-Disclosure Agreement (NDA) zugänglich gemacht wurden. Midnight Blue gelang das Reverse-Engineering mehrere kryptographischer Primitive wie dem TETRA Authentication Algorithm (TAA1) oder den TETRA Encryption Algorithmen TEA1, TEA2 und TEA3, wodurch die sogenannten TETRA:BURST Schwachstellen gefunden werden konnten.

Die verfügbaren TEA Algorithmen werden in unterschiedlichen Bereichen je nach Verwendungszweck eingesetzt. Der TEA1 und TEA4 Algorithmus werden für industrielle Zwecke genutzt. Alle TEA Algorithmen

* 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.

verwenden einen 80-Bit Schlüssel. Eine der gefundenen Schwachstellen, welche die Schlüssellänge auf nur 32-Bit reduziert, befindet sich in TEA1. In TEA2 und TEA3, welche von Polizei, Rettungsdiensten und Militär verwendet werden, konnten die Forschenden keine Schwachstelle finden [HEIS2023][MNBL2023]. TEA4 wurde von den Forschenden nicht untersucht.

Es handelt sich um folgende fünf Schwachstellen [MNBL2023]:

CVE-2022-24401 - Verlust der Vertraulichkeit und Authentizität

Der Initialisierungs Vektor (IV) des Air Interface Encryption (AIE) Keystream-Generators hängt von unverschlüsselten Broadcast Informationen ab. Dadurch sind Orakelanganriffe möglich mit denen die Kommunikation entschlüsselt werden könnte.

CVE-2022-24402 - Verlust der Vertraulichkeit und Authentizität

Durch ein schwaches Design des TEA1-Algorithmus wird die ursprünglichen Schlüsselgröße von 80-Bit auf eine Schlüsselgröße von 32-Bit reduziert. Dies ermöglicht Angreifenden das Entschlüsseln der Kommunikation in Echtzeit sowie das Injizieren von manipulierten Nachrichten.

CVE-2022-24403 - Benutzer Deanonymisierung und Ortung

Das kryptografische Schema, das zur Verschleierung der Funkidentitäten verwendet wird, hat eine schwache Gestaltung, die es Angreifenden ermöglicht, Geräte zu deanonymisieren und zu verfolgen.

CVE-2022-24404 - Verlust der Authentizität

Das Fehlen einer Verschlüsselungsauthentifizierung auf Air Interface Encryption (AIE) ermöglicht Verformbarkeitsangriffe auf die verschlüsselten Daten.

CVE-2022-24400 - Verlust der Authentizität und Teile der Vertraulichkeit

Eine Schwachstelle im Authentifizierungsalgorithmus ermöglicht es Angreifenden, den abgeleiteten Chiffrierschlüssel (DCK) auf 0 zu setzen.

Bewertung

Die CVE-2022-24401 basiert auf einer grundsätzlichen Schwäche der XOR-Verschlüsselung bei mangelndem Replay-Schutz. Das konkret beschriebene Angriffsszenario erscheint theoretisch möglich und impliziert eine theoretische Gefährdung der Vertraulichkeit. Midnight Blue hat einen Proof-of-Concept entwickelt und eine Demonstration bereitgestellt [MNBL2023].

Die CVE-2022-24402 offenbart eine fundamentale Schwäche des TEA1-Algorithmus. Der Aufwand für die Realisierung des Angriffs wird als gering bewertet. Die reduzierte Schlüsselkomplexität mit 32-Bit kann mittlerweile von handelsüblichen Hardware in kurzer Zeit gebrochen werden. Dies erlaubt es Angreifenden die Vertraulichkeit und Authentizität von Nachrichten zu untergraben und so möglicherweise gefälschte Befehle an Geräte zu senden. Midnight Blue hat einen Proof-of-Concept entwickelt und eine Demonstration bereitgestellt [MNBL2023].

Die Schwachstelle CVE-2022-24403 ermöglicht es, Geräteidentitäten zu entschlüsseln. Somit könnten Angreifende die Bewegung bestimmter Geräte nachvollziehen.

Die Schwachstelle CVE-2022-24404 ermöglicht es Angriffe auf die Verformbarkeit der verschlüsselten Daten vorzunehmen. Durch das Fehlen eines kryptographischen Integritätsschutzes könnten TETRA-Geräte manipulierte Nachrichten akzeptieren.

Die Ausnutzung der CVE-2022-24400 ist theoretisch möglich, stellt jedoch aufgrund starker Voraussetzungen – insbesondere einer notwendigen Vorhersage eines Zufallswerts – aus praktischer Sicht eine geringe Bedrohung dar.

In Deutschland wird TEA1 nicht in Behörden und Organisationen mit Sicherheitsaufgaben (BOS) eingesetzt. Stattdessen wird TEA2 verwendet und zusätzlich mithilfe der BOS-Sicherheitskarte eine Ende-zu-Ende-Verschlüsselung umgesetzt.

Die Vertraulichkeit der Kommunikation des Digitalfunks BOS ist ausdrücklich nicht beeinträchtigt, da die zum Einsatz kommende Ende-zu-Ende-Verschlüsselung nicht betroffen ist.

Eine Gefährdung von kommerziellen Anwendungen, z. B. im Bereich industrieller Steuerungssysteme kann ohne weitere Gegenmaßnahmen nicht ausgeschlossen werden. Insbesondere CVE-2022-24402 könnte es Angreifenden ermöglichen, Datenverkehr zu manipulieren und falsche Befehle an Systeme und Komponenten zu versenden.

Eine zielgerichtete Ausnutzung der Schwachstellen ist möglich, jedoch müssen Angreifende sich in die Nähe des Zieles begeben. Aktive Angriffe, also das Einbringen von nicht authentischen Nachrichten, benötigen eine ausreichende Signalstärke und spezialisierte Ausrüstung. Insbesondere Angriffe, die eine Basisstation imitieren, müssen eine Signalstärke erreichen, die deutlich größer ist als die der originalen Basisstation.

Dadurch, dass die Schwachstellen bereits seit 2021 den Herstellern bekannt sind, konnten sie für betroffene Geräte Softwareupdates bereitstellen, die die entsprechenden Schwachstellen beheben.

Es existieren aktuell keine Hinweise auf eine aktive Ausnutzung der Sicherheitslücken in Deutschland.

Maßnahmen

In kommerziellen Anwendungen kann in Deutschland TEA1 zum Einsatz kommen. Betreiber Kritischer-Infrastrukturen sollten aufgrund der veröffentlichten Schwachstellen, ihre TEA1 verschlüsselten TETRA Verbindungen einer erneuten Risikobetrachtung unterziehen. Grundsätzlich können unsichere Verbindungen mithilfe einer geeigneten Ende-zu-Ende-Verschlüsselung abgesichert werden. Betreibern wird empfohlen, sich an die Gerätehersteller zu wenden, um zeitnah Updates zu erhalten.

Links

[MNBL2023] <https://tetraburst.com/>

[HEIS2023] <https://www.heise.de/news/Digitaler-Behoerdenfunk-Massive-Schwachstellen-bei-TETRA-entdeckt-9226620.html>

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 vom BSI verwendete TLP basiert auf der Definition der TLP Version 2.0 des „Forum of Incident Response and Security Team“ (FIRST). Es dient der Schaffung von Vertrauen in Bezug auf den Schutz ausgetauschter Informationen durch Regelungen der Weitergabe. Eine unbefugte Weitergabe kann eine Verletzung der Vertraulichkeit, eine Rufschädigung, eine Beeinträchtigung der Geschäftstätigkeit oder datenschutzrechtliche Belange zur Folge haben. Im Zweifelsfall ist immer in Absprache mit dem Informationsersteller zu handeln.

2) Welche Einstufungen existieren?

- **TLP:CLEAR: Unbegrenzte Weitergabe**

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

- **TLP:GREEN: Organisationsübergreifende Weitergabe**

Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden. Eine Weitergabe von den Partnerorganisationen an weitere Personen oder Organisationen ist solange zulässig, wie diese weiteren Empfänger derselben Nutzergruppe (bspw. Angehörige der Cybersecurity-Community) angehören.

- **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Weitergabe**

Der Empfänger darf die Informationen, welche als TLP:AMBER gekennzeichnet sind, an seine Partner weitergeben, soweit diese die Informationen zur Schadensreduktion oder dem eigenen Schutz benötigen. Eine Weitergabe von den Partnern an Dritte ist nicht erlaubt und auch innerhalb der Partnerorganisationen gilt das Prinzip „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.

TLP:AMBER+STRICT: Eingeschränkte interne Weitergabe

Die Einstufung von Informationen als TLP:AMBER+STRICT beschränkt die Weitergabe ausschließlich auf die Organisation des Empfängers. Jegliche Weitergabe darüber hinaus ist untersagt. Es gilt „Kenntnis nur, wenn nötig“. 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. TLP:RED eingestufte Informationen sollten möglichst mündlich oder persönlich übergeben werden.

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:CLEAR eingestufte Informationen aus dem Kreis der Verpflichteten.

Hinweis zu Upload-, Prüf- und Übersetzungsdiensten

TLP-ingestufte Dokumente (außer TLP:CLEAR) dürfen nicht auf Plattformen Dritter (wie Virustotal, Übersetzer, etc.) hochgeladen werden, da die Dokumente dort ggf. Dritten zugänglich gemacht werden.