Tartu Ülikool

Arvutiteaduse instituut

CVE-2020-10263: Kõlari ülevõtmine

Uurimistöö

Autor: Johannes Tammerand

Tartu 2024

1 Taust

CVE-2020-10263 turvaauk avaldub kõlaritel *XIAOMI XIAOAI speaker Pro LX06 1.52.4*, mille kaudu on võimalik läbi UART (*Universal Asynchronous Receiver/Transmitter*) ühenduse logida sisse kõlari juurkasutajasse ilma paroolita. Juurkasutajana on võimalik saada ligi kõigele, mis kõlaris on: nt. wifi paroolid, kõlarisse salvestatud helifailid. Lisaks on võimalik läbi kõlari infrapuna emitteri saadeta enda sõnumeid ning ka läbi kõlari vahetada kohaliku ruuteri sätteid. Lisaks on kõlaril ka helituvastuse funktsioon, mille kaudu saab kasutaja sellega suuliselt suhelda. Läbi turvaaugu on võimalik ka seda muuta või seal toimuvaid vestlusi salvestada ning edastada. [1]

2 Turvaauk

2.1 Eeltingimused

Turvaaugu avaldumise ainsad eeltingimused on, et ründajal on füüsiline ligipääs ruuterile, ning et neil on vajalik riistavara ruuteriga läbi UART ühendust luua.

2.2 Turvaaugu avaldumine

CVSS v3.1 Baas skoor (*Base Score*) : 6.8 [3]

CVSS v3.1 vektor: CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H [3]

Ründevektor (*Attack Vector*) AV:P – Turvaauk on kasutatav vaid siis, kui ründajal on füüsiline ligipääas ohvri seadmele.

Ründekeerukus (*Attack Complexity*) AC:L – Turvaaugu kasutamiseks pole vaja eriliste tingimuste olemasolu.

Privileegide vajadus (*Privileges Required*) PR:N – Turvaaugu kasutamiseks pole masinas ründajal mingisuguseid privileege vaja.

Kasutaja tegevused (*User Interaction*) UI:N – Ohvril pole vaja midagi teha, et ründaja saaks turvaauku täielikult kasutada.

Käsitlusala (*Scope*) S:U – Ründajal on ligipääas vaid rünnatud kõlarile.

Konfidentsiaalsus (*Confidentiality*) C:H – Suur kogus rünnatud masina andmetest on ründajale kättesaadavad.

Terviklus (*Integrity*) I:H – Ründaja saab kustutada või muuta kõiki talle kättesaadavaid andmeid.

Kättesaadavus (*Availability*) A:H – Ründaja saab kõik, mis talle kättesaadav, ohvri jaoks kättesaadamatuks muuta.

Turvaaugule on antud ka CWE kood CWE-306, mis tähendab, et tootel puudub autentimine kriitilisel funktsioonil. [3]

2.2 Turvaaugu põhjus

Turvaaugu põhjuseks on see, et kõlarit juhtiv operatsioonisüsteem ei autendi sisenemist UART interaktsioonivahendi kaudu, mis laseb ründajal vabalt sisse logida juurkasutajana, millena on neil täielik kontroll terve masina tarkvara üle. [1]

Turvaauguga kõlaril ei saa midagi teha, et turvaauku vältida. Kuid, kuna turvaaugu kasutamiseks on vajalik füüsiline ligipääas seadmele ning auk ise on vähetuntud, pole ostetud kõlarite kohta üldiselt vaja muretseda, eriti kui seda polnud enne kättesaamist pakist eemaldatud.

3 Mõju ja turvaaugu kõrvaldamine

3.1 Mõju varadele

Läbi turvaaugu on ründajal võimalik mõjutada kõike kõlari tarkvaras. Näiteks on võimalik saada kätte Wi-Fi parool ning SSID (võrgu identifikaator), mis on hoitud krüpteerimata kujul ning näha kõlari ja kasutaja vahelisi vestlusi. Lisaks on võimalik kõlarisse enda koodi sisestada, mille saab nt. muuta seda, mida kõlar kasutajalt küsib ning ka salvestada vestluste helifaile ning neid mujale saata. Kõlaril saab ka käivitada SSH (Secure Shell) või Telnet teenused, mille läbi on võimalik ka kaugelt turvaauku ära kasutada. Kõlar on varustatud ka infrapuna emitteriga, mille kaudu on ründajal võimalik saata enda tehtud signaale. Viimaks on võimalik ka kõlari läbi muuta ruuteri konfiguratsiooni. [1, 2]

3.2 Turvaaugu parandamine

Turvaaugu parandamise kohta pole infot leida, seega võib eeldada, et selle kohta pole midagi tehtud. Selle põhjuseks võib olla see, et kõlari tegijate arust pole selle parandamine aega väärt või, et kõlari tarkvara pole võimalik uuendada.

3.3 Turvaaugu tegelik ärakasutatavus

Midagi turvaaugu kasutamise kohta ma ei leidnud, ainuke allikas selle kohta on konseptsiooni tõestus (PoC), kus turvaaugu leidja, Hiina Kaohsiung tehnoloogiaülikooli tudeng, demonstreeris kõike, mida ma seni olen turvaaugu kohta maininud. [1, 2]

Augu avastamise kuupäeva seal kirjas pole, kuid avastaja poolt loodud artikkel avaldati esimest korda 7. aprillil 2020.

Kasutatud allikad

[1] Jian-Xian Li. CVE-2020-10263, 2020. https://github.com/Jian-Xian/CVE-POC/blob/master/CVE-2020-10263.md (06.05.2024)

[2] Jian-Xian Li. XIAOMI XIAOAI speaker Pro' voice achieve social engineering attacks, 2020. https://www.youtube.com/watch?v=Cr5DupGxmL4 (06.05.2024)

[3] NIST. CVE-2020-10263 Detail, 2020. https://nvd.nist.gov/vuln/detail/CVE-2020-10263 (06.05.2024)

Lisa 1 – Litsents

Mina, **Johannes Tammerand**, annan Tartu Ülikoolile loa (lihtlitsentsi) minu loodud uurimustööd teemal **CVE-2020-10263: Kõlari ülevõtmine** avalikult eksponeerida kuni aastani 2029, k.a.

Johannes Tammerand

6. mai 2024. a.