Check Point hoiatab: meediapleieri subtiitrite kaudu saab häkker arvuti üle võtta

9 aastat tagasi - 24.05.2017 Autor: AM

Arvutiturvalisuse maailmast tuleb jälle üks uudis, mis muudab meie arusaamist IT-turvalisusest. Turvatarkvara tootja Check Point postitas teate "Hacked in Translation", milles nad väidavad, et on avastanud võimaluse subtiitrifailide kaudu tuntud meediapleierite nõrkust kasutades ohvri arvuti eemalt üle võtta. Lisaks saavad pahalased manipuleerida subtiitrisaitide (nagu Opensubtitles.org) edetabeleid, et nakatavat koodi sisaldavad subtiitrid ettepoole tõsta.

Paraku pole Check Point avaldanud, kuidas tavaliselt tekstifailina arvutisse saabuvad subtiitrifailid pahavarana töötavad. Firma põhjendab seda vajadusega oodata, kuni kõik enamlevinud meediapleierid on selle ründe vastu oma uues tarkvaraversioonis kaitse väljastanud.

Kõik levinud meediapleierid ja viirusetõrjed käsitlevad subtiitrifaile ohututе tekstifailidena, mis ei saa sisaldada midagi kahjulikku peale teinekord liiga vürtsikate kõnekeeleliste väljendite. Kuid nendega turvatarkvara tavaliselt ei tegele, kui pole just kasutusel vanemliku järelevalve filtrit. Seekordne ründevektor aga kasutabki seda näilist turvalisust ja kontrollimatust ära - süütu teksti vahele on peidetud midagi, millest Check Point veel ei räägi, kuid mis võib avada uksed väljaspool asuvale ründajale. Uksed avatakse nii laialt, et peale nakatumist saab ründaja ohvri arvutis teha, mida tahab. Ohtu suurendab veel see, et paljud pleierid otsivad ise vajalikud subtiitrid ja laadivad need filmivaataja arvutisse automaatselt alla.

Turvaauk leiti kolmest kõige levinumast meediapleierist: VLC, Kodi (XBMC), Popcorn-Time ja strem.io on nakatatavad. Kokku võivad ohus olla ligi 200 miljonit arvutit, nutitelerit ja mobiilset seadet.

Mõned meediamängijad on juba saanud uuenduse, mõned mitte. Praegune seis on selline:

- **PopcornTime** – turvauuendus on tehtud, selle saab kodulehelt alla laadida: https://ci.popcorntime.sh/job/Popcorn-Time-Desktop/249
- **Kodi** – saadaval on uuenduse lähtekood, mida oskavad programmiks kompileerida asjatundjad. Allalaadimiseks valmisversiooni veel ametlikul kodulehel pole.

Lähtekood asub siin: https://github.com/xbmc/xbmc/pull/12024

- **VLC** – maailma üks populaarseimatest meediapleieritest on uuenduse väljastanud ja see olevat ka kodulehelt saadaval (ehkki eraldi märget turvaprobleemi kõrvaldamise kohta tootja lehel pole). Link: http://get.videolan.org/vlc/2.2.5.1/win32/vlc-2.2.5.1-win32.exe
- **Stremio** – samuti ametlikult kõrvaldatud turvaauguga versioon on kodulehelt www.strem.io allalaetav. Teadet subtiitrihäki kohta pole.

Turvaohuks on märgitud "*Subtitles Remote Code Execution*". Kuidas see täpsemalt välja näeb, selgub allolevast videost.

- Uudised

- Androidiblog
- Tahvelarvutid
- Tarkvara
- Turvalisus

Pilt