Tahad teenida kuni miljoni? Siis leia Whatsappist turvanõrkus

9 kuud tagasi - 04.08.2025 Autor: AM

Meta (see Facebooki firma) pakub Pwn2Own Ireland 2025 häkkimisvõistlusel WhatsAppi nõrkuste leidmise eest kuni 1 miljon dollarit.

Trend Micro Zero Day Initiative´i (ZDI) korraldatav Pwn2Own on maailmakuulus võistlus, kus "valge mütsiga" ehk *White hat* häkkerid (eetiline häkker, kes otsib süsteemist nõrkusi eesmärgiga neid parandada) demonstreerivad erinevate tarkvara- ja riistvarasüsteemide turvaauke. Nii tahetakse suurendada süsteemide turvalisust, avastades nõrkused enne, kui pahatahtlikud ründajad neid ära kasutavad.

Sel aastal on võistluse fookuses mitmed kategooriad, sealhulgas mobiiltelefonid, nutikad koduseadmed, printerid ja kantavad seadmed (*wearables*).

Eraldi on välja toodud aga WhatsApp, mille murdmise eest pakutakse suurimaid rahalisi auhindu.

Mida tähendavad Pwn2Owni auhinnad?

Erinevate WhatsAppi turvanõrkuste avastamise eest saab erinevaid auhindu.

Target	Options	Cash Prize	Master of Pwn Points
WhatsApp	0-Click Remote Code Execution	$1,000,000 (USD)	100
	1-Click Remote Code Execution	$500,000 (USD)	50
	Remote 0-Click Account Take-over	$150,000 (USD)	15
	Remote 0-Click Access to Microphone or Video Feed	$130,000 (USD)	13
	Remote 0-Click Access to User Sensitive Data	$130,000 (USD)	13
	Remote One-Click Access to User Sensitive Data	$130,000 (USD)	13
	Zero-Click Impersonation of Other Users in Chats	$50,000 (USD)	5

Mõistmaks, mis teeb ühest turvaaugust väärtuslikuma kui teisest, on oluline aru saada, mida need terminid tähendavad.

- **0-Click (Zero-Click) :** See on kõige ohtlikum ja väärtuslikum turvanõrkus, mis ei vaja rünnaku sooritamiseks mingit kasutajapoolset tegevust. Näiteks võib ründaja saata ohvrile spetsiaalselt koostatud sõnumi või videokõne, mis ilma ohvri igasuguse interaktsioonita (nt lingi avamine, faili allalaadimine) suudab seadme üle võtta. Sellise haavatavuse eest pakutakse 1 miljon dollarit, kuna see on äärmiselt ohtlik ja annab ründajale täieliku kontrolli ohvri seadme üle.
- **1-Click (One-Click):** See on turvanõrkus, mis nõuab ohvrilt rünnaku käivitamiseks üht konkreetset tegevust, näiteks lingi avamist, faili allalaadimist või pildile klikkimist. Kuigi see on vähem ohtlik kui 0-Click, on see siiski väga tõsine turvaprobleem, mille eest pakutakse 500 000 dollarit.
- **Remote Code Execution (RCE):** See tähendab kaugkäivitatavat koodi. Ehk siis ründaja saab rünnaku tulemusena ohvri seadmes käivitada omaenda pahatahtlikku koodi. See on kõige tõsisem oht, kuna annab ründajale täieliku kontrolli seadme üle, võimaldades varastada andmeid, installeerida lunavara või teha muid pahatahtlikke tegevusi.
- **Account Take-over:** See haavatavus võimaldab ründajal ilma ohvri teadmata võtta üle tema WhatsAppi konto. See annab ründajale ligipääsu kõikidele vestlustele ja kontaktidele, võimaldades tal ohvri nimel suhelda ja pettusi sooritada.

- **Access to Microphone or Video Feed:** See nõrkus võimaldab ründajal ilma ohvri loata ligi pääseda seadme mikrofonile või kaamerale. Ründaja saab kuulata vestlusi või jälgida ohvri tegevusi reaalajas.
- **Access to User Sensitive Data:** See nõrkus annab ründajale ligipääsu tundlikele andmetele, mis on seadmesse salvestatud. See võib hõlmata näiteks kontaktide nimekirja, asukohaandmeid või muid isiklikke andmeid.
- **Impersonation of Other Users in Chats:** See haavatavus võimaldab ründajal saata ohvri nimel sõnumeid teistele kasutajatele või saata sõnumeid, mis tunduvad pärinevat kelleltki teiselt. See võib olla ohtlik andmepüügi ja sotsiaalmanipulatsiooni kampaaniate puhul.

Pwn2Owni võistlused on oluline osa küberturvalisuse ökosüsteemist. Leides ja parandades need nõrkused enne pahalaste poolt nende ärakasutamist, aitavad White hat häkkerid muuta interneti ja tarkvarasüsteemid turvalisemaks. Meta otsus sponsoreerida WhatsAppi exploitide leidmist näitab ettevõtte pühendumust platvormi turvalisuse parandamisele.

Võistlus ise toimub 21.–24. oktoobril 2025. Mobiilikategoorias saab samuti häkkida Samsung galaxy S25, Google Pixel 9 ja Apple iPhone 16 telefone. Seda võistlust on veidi kohandanud, lisades telefonidele uue USB-rünnakuvektori, mis näitab, mis võib siis juhtuda, kui ründajal on füüsiline juurdepääs seadmele.

Eelmisel aastal anti võistlusel välja 1 066 625 USA dollarit enam kui 70 unikaalse 0-päevase haavatavuse eest. Sel aastal loodetakse samuti head saaki, eriti kui laual on miljoni dollari suurune "peavõit".

- Uudised

- Tarkvara
- Turvalisus

Pilt


WhatsApp Messenger
Version 2.17.427
© 2010–2017 WhatsApp Inc.
All rights reserved.
LIZENZEN