Zraniteľnosti v aplikácii eID klient

Na prelome februára a marca 2019 boli identifikované viaceré zraniteľnosti v aplikácii eID klient, ktoré bolo možné za určitých podmienok zneužiť na vzdialené spustenie škodlivého kódu alebo na modifikáciu súborov na zariadení. Vládna jednotka CSIRT tieto zraniteľnosti preverila a v súčinnosti s Ministerstvom vnútra, Národnou agentúrou pre sieťové a elektronické služby a dodávateľom aplikácie spolupracovala pri riešení incidentu. V krátkom čase boli identifikované zraniteľnosti odstránené. Taktiež bola Vládnou jednotkou CSIRT vykonaná bezpečnostná analýza aplikácie, počas ktorej boli identifikované ďalšie zraniteľnosti nižšej závažnosti. Tieto zraniteľnosti boli opravené následnou bezpečnostnou aktualizáciou aplikácie.

Úvod

Aplikácia eID klient slúži na elektronickú identifikáciu majiteľa občianskeho preukazu s čipom, ktorá slúži na prihlasovanie sa na portál www.slovensko.sk, do elektronických schránok alebo na iný špecializovaný portál verejnej správy. Vládna jednotka CSIRT prijala dňa 28.2.2019 hlásenie od spoločnosti BinaryHouse o identifikácii zraniteľností v produkte eID klient vo verzii 3.0.0 a nižšie. Vzhľadom na závažnosť nahlásených zraniteľností a potenciálne ohrozenú veľkú skupinu obyvateľstva bola v spolupráci Vládnej jednotky CSIRT, MINV, NASES a dodávateľa aplikácie pripravená a otestovaná bezpečnostná aktualizácia opravujúca tieto zraniteľnosti.

Opis činnosti

Aplikácia eID klient obsahuje jednoduchý open-source webserver CivetWeb odvodený od webservera Mongoose. Tento webserver sprostredkováva komunikáciu medzi webovými aplikáciami využívajúcimi eID a lokálnou inštaláciou programu eID klient. Počúva na porte 15480 a počas komunikácie súvisiacej s eID naň smerujú požiadavky určené pre localhost. Avšak vo verziách pre operačné systémy Linux a MacOS tento webserver nepočúva iba na localhoste, ale na všetkých IP adresách daného zariadenia (0.0.0.0), v dôsledku čoho je možné nižšie uvedené zraniteľnosti využiť aj vzdialene, bez interakcie používateľa.

Webserver CivetWeb v aplikácii eID klient je implementovaný tak, aby špeciálne spracovával iba požiadavky na určité URL (endpointy), avšak v dôsledku chybnej implementácie je štandardným spôsobom spracovávaná aj požiadavka smerovaná na inú URL. Súčasťou štandardného spracovávania požiadaviek je aj spracovávanie metód PUT a DELETE a taktiež aj spracovávanie a zobrazovanie dynamického obsahu pomocou CGI/SSI. Zároveň má uvedený webserver nastavený ako domovský adresár pre webové stránky (DocumentRoot) adresár, v ktorom sú prítomné používateľské súbory (napr. v prípade OS Linux je to domovský adresár používateľa), teda požiadavky s vhodnou URL môžu vyústiť do manipulácie s používateľskými súbormi.

DELETE

Pomocou metódy DELETE je možné zmazať súbor uvedený v URL adrese.

PUT

Metóda PUT sa využíva na uloženie údajov z požiadavky do súboru v URL adrese. Kvôli implementácii však v tomto prípade neprebehne uloženie všetkých dát do súboru, iba vytvorenie prázdneho súboru uvedeného v URL adrese. V prípade, že daný súbor existuje, jeho obsah sa vymaže a vznikne prázdny súbor.

SSI/CGI

Pomocou SSI je možné vykonávať obsah zo súborov s príponami .shtml a .shtm, pomocou CGI podporuje webserver spúšťanie súborov s príponami .cgi, .pl a .php. Keďže integrovaný webserver má nastavený DocumentRoot do adresára s používateľskými súbormi, je možné takto spúšťať súbory s vyššie

uvedenými príponami. V kombinácii s automatickým sťahovaním súborov tak môže útočník zneužiť túto zraniteľnosť na podvrhnutie a spustenie súboru so škodlivým obsahom.

Na úspešnú exploitáciu uvedených zraniteľností je v prípade OS Windows potrebná interakcia používateľa, napr. návšteva stránky vo webovom prehliadači, v dôsledku čoho sa spustí javascript, ktorý vykoná dopyt na lokálny webserver eID klienta. Na takýto útok je potrebné použiť ešte aj ďalšiu techniku na obídenie blokovania medzidoménových požiadaviek, avšak takéto techniky existujú.

Na úspešnú exploitáciu uvedených zraniteľností eID klienta pre OS Linux a MacOS nie je potrebná interakcia používateľa. V prípade, že nie je nastavený lokálny Firewall, takéto požiadavky môže útočník poslať na IP adresu zariadenia.

Zraniteľné systémy

Program eID klient do verzie 3.0.0 vrátane

Závažnosť zraniteľnosti

Kritická

Možné škody

Vzdialené vykonávanie škodlivého kódu
Modifikácia informácií (vymazanie súborov alebo ich obsahu)

Odporúčania

Aktualizovať aplikáciu eID klient na verziu opravujúcu zraniteľnosť. Táto aktualizácia bola vynútená a mala by prebehnúť automaticky, pokiaľ sa tak z nejakého dôvodu nestalo, je potrebné aktualizovať ručne na verziu minimálne 3.1.2 pre OS Windows, 3.0.3 pre OS Linux, prípadne aktuálnu verziu 3.2 pre všetky OS v čase písania tejto správy.

Riešenie incidentu

28.2.2019 (štv) – Vládna jednotka CSIRT.SK prijala hlásenie od spoločnosti Binary House o identifikácii zraniteľností

1.3.2019 (pia) – prebehlo stretnutie medzi zástupcami Vládnej jednotky CSIRT.SK, NASES, MINV a dodávateľa aplikácie eID. Bola vydaná verzia 3.1.2 pre OS Windows a verzia 3.0.2 pre OS Linux (ktorá ale obsahovala chybu pri spúšťaní aplikácie, ktorá bola opravená vo verzii 3.0.3)

2.-3.3.2019 (so, ne) – Vládna jednotka CSIRT vykonala bezpečnostnú analýzu aktuálnych verzií eID, v rámci ktorej identifikovala ďalších 10 potenciálnych zraniteľností nižšej závažnosti; automatická aktualizácia zraniteľných verzií aplikácie eID klient

4.3.2019 (pon) – publikovaná tlačová správa na stránke MINV

24.6.2019 (pon) – po uplynutí ochrannej lehoty zverejnené detaily o identifikovaných zraniteľnostiach, tlačová konferencia a poďakovanie etickým hackerom zo spoločnosti Binary House

Poďakovanie

Vládna jednotka CSIRT týmto vyjadruje poďakovanie pánovi Marekovi Alakšovi zo spoločnosti Binary House za identifikovanie a zodpovedné nahlásenie zraniteľností aplikácie eID klient.

Zdroje

- https://www.csirt.gov.sk/
- https://www.slovensko.sk/sk/slovnik/detail/_eid-klient
- https://github.com/civetweb/civetweb
- https://www.minv.sk/?tlacove-spravy&sprava=pouzivatelom-e-sluzieb-automaticky-aktualizujeme-aplikaciu-pre-elektronicky-obciansky-preukaz