MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Keď renderovanie bolí: Premena SVG na útok DoS v prehliadači v OTRS

CVE-2026-48208

Vytvoril: CSIRT.SK
Ministerstvo investícií, regionálneho rozvoja a informatizácie SR
Pribinova 25
811 09 Bratislava

Dátum vzniku: Marec 2026

TLP: Clear

Úvod

Moderné webové aplikácie často vychádzajú z predpokladu, že na bezpečné zobrazenie nedôveryhodného obsahu stačí vypnúť JavaScript.

Čo sa však stane, keď sa samotný prehliadač stane prostredím na spúšťanie kódu?

V tomto článku sa zaoberáme zraniteľnosťou vedúcou k nedostupnosti služby v systéme OTRS, ktorá vyplýva zo spôsobu zobrazenia obsahu tiketu. Vložením špeciálne upraveného obsahu SVG do tiketu môže útočník spôsobiť zrútenie karty prehliadača agenta pri jej zobrazení.

Tento útok nevyžaduje JavaScript, obchádza politiku Content Security Policy (CSP) a spočíva výlučne na správaní prehliadača pri vykresľovaní.

Kľúčový problém

Jadrom tejto zraniteľnosti je nesúlad medzi tým, čo aplikácia považuje za „bezpečný obsah“, a tým, čo je prehliadač schopný spracovať.

OTRS vykresľuje obsah HTML priamo v rozhraní tiketu. To zahŕňa aj vložené prvky SVG.

Hoci CSP zabraňuje spúšťaniu skriptov, nebráni prehliadaču v parsovaní a vykresľovaní zložitých štruktúr SVG.

Niektoré konštrukcie SVG môžu počas vykresľovania spôsobiť nadmernú spotrebu zdrojov alebo nestabilitu.

Kľúčový postreh

- Aplikácia blokuje vykonávanie kódu. Prehliadač však naďalej vykonáva logiku vykresľovania.

Hlavná príčina

Hlavnou príčinou nie je prítomnosť aktívnych skriptov, ale chýbajúce obmedzenia týkajúce sa **zložitosti obsahu, ktorý sa má vykresliť**.

Aplikácia vychádza z predpokladu, že:

- Blokovanie JavaScript je dostatočné
- Renderovanie obsahu je principiálne bezpečné

Oba predpoklady prestávajú platiť pri spracovaní zložitých SVG vstupov.

Prečo je to „podprahové“

Nejedná sa o typickú chybu typu XSS.

Je to:

- **Odmietnutie služby (DoS) založené na renderovaní**
- Spúšťané **platným obsahom, ktorý spĺňa štandardy**
- Spôsobené **nesprávnym využívaním vnútorných mechanizmov prehliadača, nie logikou aplikácie**

To ho robí obzvlášť nebezpečným, pretože:

- Nie je potrebný žiadny zjavný „škodlivý“ obsah
- CSP vyvoláva falošný pocit bezpečia
- Tento problém sa prejavuje iba pri vykresľovaní obsahu

Scenár útoku

Útok využíva bežné funkcie systému OTRS.

1. Útočník pošle e-mail obsahujúci špeciálne vytvorený obsah vo formáte SVG
2. OTRS automaticky vytvorí tiket na základe e-mailu
3. Pracovník otvorí tiket vo webovom rozhraní
4. Prehliadač sa pokúsi vykresliť SVG
5. Karta sa zrúti alebo prestane reagovať

Kľúčové zistenie

- Nie je potrebné overenie identity
- Okrem otvorenia tiketu nie je potrebná žiadna interakcia zo strany používateľa
- Nevyžaduje sa žiadne skriptovanie

Dopad

V zasiahnutých prostrediach môže útočník:

- Spôsobiť zlyhanie kariet prehliadača u agentov
- Narušiť pracovné postupy pri spracovaní tiketov
- Opakovane vyvolávať odmietnutia služby prostredníctvom automatického vytvárania tiketov

V prostrediach s automatizovaným načítaním e-mailov sa tento efekt môže ešte znásobiť:

- Je možné vygenerovať viacero škodlivých tiketov
- Môže to ovplyvniť viacerých agentov súčasne

V skratke:

➢ Útočník môže na diaľku obmedziť alebo narušiť operácie podporny bez toho, aby musel spustiť jediný riadok kódu JavaScript.

Prečo CSP nepomáha

Content Security Policy je určená na kontrolu **načítavania zdrojov a vykonávania skriptov**.

Avšak:

- Vykresľovanie SVG je povolené ako súčasť štandardného spracovania HTML
- Na tento útok nie sú potrebné žiadne externé zdroje
- Nevykonávajú sa žiadne skripty

V dôsledku toho:

➢ CSP úspešne blokuje nesprávny model hrozby.

Overenie koncepcie (prehľad)

Cieľ

Preukázať, že samotné vykresľovanie obsahu SVG môže viesť k nestabilite prehliadača.

Hlavná myšlienka

Cez e-mail je do tiketu vložený špeciálne vytvorený obsah SVG.

Keď sa tiket otvorí:

- Prehliadač parsuje súbor SVG
- Vykresľovanie spôsobuje nadmerné zaťaženie procesora
- Karta sa zrúti alebo prestane reagovať

Doručenie

Obsah je možné doručiť prostredníctvom štandardných procesov prepojenia e-mailu s tiketom.

Poznámka

Táto zraniteľnosť nezávisí od:

- Vykonaní kódu JavaScript
- Externých zdrojov
- Interakcia používateľa nad rámec prezerania tiketu

Kompletný skript na overenie koncepcie (PoC)

Kompletný skript na overenie funkčnosti koncepcie je k dispozícii tu:

https://github.com/Habuon/CVE-2026-48208

Aspekty detekcie

Detegovanie tohto problému môže byť náročné:

- Žiadne logy nenaznačujú zneužitie
- Nedochádza k spusteniu žiadneho skriptu
- Poruchy sa prejavujú ako zlyhania na strane klienta

Indikátory môžu obsahovať:

- Pracovníci hlásia nestabilitu prehliadača pri otváraní tiketov
- Opakované zlyhania súvisiace s konkrétnymi hláseniami

Lekcie obrany

Táto zraniteľnosť poukazuje na niekoľko dôležitých ponaučení:

1. Renderovanie predstavuje útočnú plochu

Zobrazovanie nedôveryhodného obsahu nie je pasívny proces. Spúšťa zložitú logiku prehliadača..

2. CSP nie je to úplná obrana

Blokovanie JavaScriptu neodstraňuje všetky formy zneužitia na strane klienta.

3. Považujte SVG za aktívny obsah

SVG nie je len formát obrázkov — je to programovateľný systém vykresľovania.

4. Sanitizujte nad rámec skriptov

Bezpečnostné opatrenia musia zohľadňovať zložitosť štruktúry a vykresľovania, nielen spustiteľný kód.

Stratégie mitigácie

Odporúčané spôsoby mitigácie zahŕňajú:

- Odstráňte alebo deaktivujte vložený obsah SVG v tele tiketov
- Dôkladne očistite prvky a atribúty SVG
- Vykresľujte nedôveryhodný obsah v izolovaných iframe
- Pred zobrazením konvertujte SVG do bezpečných rastrových formátov

Zverejnenie informácií

Táto chyba bola zodpovedne nahlásená bezpečnostnému tímu OTRS Product Security Team prostredníctvom procesu koordinovaného oznamovania.

Časová línia

- **2026-03-29 —** Zraniteľnosť objavená počas výskumu zobrazovania tiketov v systéme OTRS a útočných plôch na strane prehliadača.
- **2026-03-30 —** Problém bol súkromne nahlásený bezpečnostnému tímu OTRS Security Team spolu s technickými podrobnosťami a informáciami o tom, ako sa dá problém reprodukovať.
- **2026-04-09 —** Dodávateľ potvrdil existenciu tejto zraniteľnosti a overil, že špeciálne upravený obsah vo formáte SVG spôsobuje odmietnutie služby.
- **2026-05-21 — C**hybe bol priradený identifikátor **CVE-2026-48208**.
- **2026-06-01 —** Koordinované zverejnenie informácií a vydanie oznámenia.

Hodnotenie dodávateľa

CVSS v4.0

High — **7.1**

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/AU:Y/R:U/RE:L/U:Amber

CVSS v3.1

Medium — **6.5**

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Záver

Táto zraniteľnosť nám pripomína, že moderná webová bezpečnosť presahuje rámec spúšťania skriptov.

Aplikácie sa často zameriavajú na zabránenie injektovania kódu, pričom prehliadajú riziká spojené so vykresľovaním komplexného, nedôveryhodného obsahu.

Nešlo o zlyhanie filtrovania.

Išlo o to, že sa nepodarilo rozpoznať, že samotné zobrazovanie môže byť zneužité.