Ranjivost WordPress dodataka

Uvod

Praćenje sigurnosnih propusta u WordPress-u i ostalim CMS-ovima važan je dio sigurnosti. Zato Vam dostavljamo ranjive dodatke i novootkrivene ranjivosti kako bismo bili sigurni da su vaše web stranice koje koriste niže spomenute dodatke i/ili teme zaštićeni/e.

Sve ranjivosti koje ste pronašli u ovome članku dobili su zakrpu na vatrozidu WebARX. To znači da ako koristite vatrozid web aplikacije WebARX, vaša je web stranica sigurna od ovih ranjivosti, ali uvijek se savjetuje ažuriranje i/ili brisanje ranjivih dodataka sa WordPress stranica.

Popis ranjivih dodataka

Authenticated Stored XSS in GistPress Plugin

Ranjivost: Ovjereno pohranjeni XSS

Ranjiva verzija: 3.0.2 i stariji

Broj pogođenih mjesta: N / A

Pročitajte više o ranjivom dodatku na:
https://github.com/bradyvercher/gistpress/commit/e3f260edb6673227b0471c74b7ab13c094411ef7

Authenticated Stored XSS in Elementor Page Builder

Ranjivost: Ovjereno pohranjeni XSS

Ranjiva verzija: 2.7.6 i stariji

Broj pogođenih mjesta: 4+ milijuna

Razina iskorištavanja: Jednostavno / zahtijeva provjeru autentičnosti

Za sve koje koriste Elementor verzije niže od 2.7.6

Pročitajte više o ranjivom dodatku na: https://labs.sucuri.net/stored-xss-in-elementor/

Critical CSRF to RCE Vulnerability in Code Snippets Plugin

Ranjivost: Kritičan CSRF za RCE

Ranjiva verzija: ispravljeno u verziji 2.14.0

Broj pogođenih web lokacija: 200 000+

Taj bi problem mogao uzrokovati potpuna preuzimanja web lokacije.

Pročitajte više o ranjivom dodatku na: https://www.webarxsecurity.com/critical-csrf-to-rce-code-snippets-plugin/

Authenticated Reflected XSS in Elementor Page Builder

Ranjivost: Ovjereno odraženi XSS

Ranjiva verzija: 2.8.5 i stariji

Broj pogođenih mjesta: 4+ milijuna

CSV Injection in Flamingo Plugin

Ranjivost: ubrizgavanje CSV-a

Ranjiva verzija: 2.1.1 i stariji

Broj pogođenih web lokacija: 500 000+

Otkrivena je ranjivost CSV ubrizgavanja u Flamingo Plugin v 2.1. Omogućuje korisniku s povlasticama niske razine da ubrizga naredbu OS-a koja će biti uključena u izvezenu CSV datoteku. To dovodi do moguće izvedbe naredbe / koda.

Pročitajte više o ranjivom dodatku na: https://fortiguard.com/zeroday/FG-VD-20-004

Missing Authorization Check In wpCentral Plugin

Ranjivost: eskalacija privilegija

Ranjiva verzija: 1.4.7 i stariji

Broj pogođenih web lokacija: 50 000+

U inačicama 1.4.7 i nižim od ovog dodatka postoji ranjivost koja omogućuje svima koji su prijavljeni s bilo kojom korisničkom ulogom eskaliranje svojih privilegija ili izmjenu / prijenos bilo koje datoteke, ili prilagodi bilo koji dodatak i komunicira sa web mjesto na mnogo drugih načina.

Pročitajte više o ranjivom dodatku na: https://www.webarxsecurity.com/wpcentral-plugin-leads-to-multiple-vulnerabilities/

Secret Login Page Disclosure in WPS Hide Login Plugin

Ranjivost: Tajno otkrivanje stranice za prijavu

Ranjiva verzija: 1.5.5 i stariji

Broj pogođenih web lokacija: 500 000+

Ranjivost u verziji 1.5.4.2 i stariji može omogućiti napadaču da pronađe i pristup tajnoj stranici za prijavu.

Pročitajte više o ranjivom dodatku na: http://www.https.com//blog.nintechnet.com/wordpress-wps-hide-login-fixed-security-issue/

Stored XSS in WP DS FAQ Plus Plugin

Ranjivost: Pohranjeno XSS

Ranjiva verzija: 1.0.354 i stariji

Broj pogođenih web lokacija: 50 000+

Authenticated Stored XSS in Calculated Fields Form Plugin

Ranjivost: Ovjereno pohranjeni XSS

Ranjiva verzija: 1.0.354 i stariji

Broj pogođenih web lokacija: 50 000+

Ovjereni korisnik s pristupom uređivanju ili stvaranju polja Obrazac može sadržavati JavaScript u polja za unos, kao što su" ime polja "i" ime obrasca "."

Unauthenticated Reflected XSS in Chained Quiz Plugin

Ranjivost: Neovjereno odraženi XSS

Ranjiva verzija: 1.1.8.2 i stariji

Broj pogođenih web lokacija: 1 000+

Plugin Chained Quiz prije 1.1.8.2 pati od Reflected XSS ranjivosti u POST parametru 'total_questions' kada korisnik završi kviz.

Kôd prihvaća parametar 'total_questions' bez izbjegavanja posebnih znakova: models / quiz.php $ output = str_replace ('{{questions}}', $ _POST ['total_questions'], $ output);

WordPress Hardening Bypass

U jezgri WordPress-a postoji ranjivost daljinskog izvršenja koda (RCE) koja zaobilazi mehanizme učvršćivanja. Ranjivost je prisutna u jezgri WordPress-a u verzijama prije 5.2.4.

Obavezno ažurirajte svoje WordPress instalacije na 5.2.4 ili noviju verziju da biste spriječili zaobilaznicu.

Pročitajte više o ranjivom dodatku na: https://blog.ripstech.com/2020/wordpress-hardening-bypass/

Authenticated Stored XSS in Contact Form Clean and Simple Plugin

Ranjivost: Ovjereno pohranjeni XSS

Ranjiva verzija: 4.7.0 i stariji

Broj pogođenih web lokacija: 20 000+

Kad korisnik ima mogućnosti administratora, zlonamjerni kôd može se poslati putem opcija dodataka.

Pročitajte više o ranjivom dodatku na: https://jrjmulder.nl/plugins/contact-form-clean-and-simple-4-7-0-authenticated-stored-xss/

Insecure Direct Object Reference (IDOR) in Ultimate Member Plugin

Ranjivost: nesigurna direktna referenca objekta (IDOR)

Ranjiva verzija: 2.1.3 i stariji

Broj pogođenih web lokacija: 100 000+

Problemi s IDOR-om koji omogućuju promjenu profila drugih korisnika i naslovnih fotografija.

Pročitajte više o ranjivom dodatku na: https://github.com/ultimatemember/ultimatemember/commit/249682559012734a4f7d71f52609b2f301ea55b1

Arbitrary PHP Execution in AccessAlly Plugin

Ranjivost: Samovoljno izvršavanje PHP-a

Ranjiva inačica: 3.3.2 i stariji

Broj pogođenih mjesta: N / A

Prije verzije 3.3.2, ovaj dodatak omogućio je proizvoljno izvršavanje PHP-a putem funkcije login_error.

DOM Cross-Site Scripting in Chatbot with IBM Watson Plugin

Ranjivost: XSS temeljen na DOM-u

Ranjiva verzija: 0.8.21 i stariji

Broj pogođenih web lokacija: 2 000+

XSS ranjivost utemeljena na DOM-u identificirana je u funkcionalnosti za chat dodatka Watson Assistant za WordPress, omogućavajući udaljenom napadaču da izvrši JavaScript u pregledniku žrtve tako što je ugurao žrtvu u lijepljenje HTML-a unutar chatbox-a.:

Authenticated Stored Cross-Site Scripting Issue in Contextual Adminbar Color Plugin

Ranjivost: Ovjeren problem pohranjene skripte na više web lokacija

Ranjiva verzija: 0,3 i stariji

Broj pogođenih web-lokacija: 40+

Authenticated Arbitrary Plugin Deactivation in 2J SlideShow Plugin

Ranjivost: Autentična proizvoljna deaktivacija dodatka

Ranjiva verzija: 1.3.40 i stariji

Broj pogođenih web lokacija: 3 000+

Nedostatak provjere autorizacije u funkciji twoj_slideshow_setup () registriranom kao AJAX poziv mogao bi omogućiti autentificiranim korisnicima s malim privilegijima da deaktiviraju proizvoljne dodatke.

Broken Authentication Leading To Unauthenticated Stored XSS in Batch-Move Posts Plugin

Ranjivost: Slomljena provjera autentičnosti koja vodi do neovlaštenog pohranjenog XSS-a

Ranjiva verzija: 1.5 i stariji

Broj pogođenih mjesta: N / A

Napadač može daljinski dodati XSS korisni teret bez autentifikacije. Payload se pokreće kada Admin posjeti stranicu postavki dodatka.

CSRF to XSS in Marketo Forms and Tracking Plugin

Dodatak je zatvoren.

Ranjivost: CSRF na XSS

Ranjiva verzija: 1.0.2 i stariji

Broj pogođenih mjesta: N / A

Reflected XSS in Chained Quiz Plugin

Ranjivost: Odbijeni XSS

Ranjiva verzija: 1.1.8.2 i stariji

Broj pogođenih web lokacija: 1 000+

Multiple Vulnerabilities in WP Database Reset Plugin

Ranjivost: Nepotvrđeno resetiranje baze podataka

Ranjiva verzija: 3.1 i stariji

Broj pogođenih web lokacija: 80 000+

Ta je mana omogućila bilo kojem neovlaštenom korisniku da resetira bilo koju tablicu iz baze podataka u početno stanje postavljanja WordPressa.

Reflected Cross-Site Scripting in LearnDash Plugin

Ranjivost: Osvrt na problem skriptiranja na više web lokacija (XSS) na polju pretraživanja [ld_profile]

Ranjiva inačica: utvrđeno u verziji 3.1.2

Broj pogođenih mjesta: N / A

Authenticated Stored XSS in Video on Admin Dashboard

Ranjivost: Ovjereno pohranjeni XSS

Ranjiva verzija: ispravljeno u verziji 1.1.4

Broj pogođenih web-lokacija: 40+

Videozapis na nadzornoj ploči administratora ranjiv je za pohranjeni XSS. Kad korisnik ima mogućnosti administratora, zlonamjerni kôd može se poslati putem opcija dodataka.

Authenticated Stored XSS in Computer Repair Shop Plugin

Ranjivost: Ovjereno pohranjeni XSS

Ranjiva verzija: fiksno u verziji 2.0

Broj pogođenih web-lokacija: 40+

Computer Repair Shop je ranjiv na pohranjeni XSS. Kad korisnik ima mogućnosti administratora, zlonamjerni kôd može se poslati putem opcija dodataka. Popravljeno u verziji 2.0.

CSV Injection in TablePress Plugin

Ranjivost: ubrizgavanje CSV-a

Ranjiva inačica: 1.10 i stariji

Broj pogođenih web lokacija: 800 000+

"Preko ranjivosti CSV ubrizgavanja zlonamjerni korisnik može prisiliti druge korisnike da izvršavaju kôd na svom računalu, na primjer, to se može koristiti za širenje zlonamjernog softvera."

CSV Injection in WooCommerce – Store Exporter Plugin

Ranjivost: ubrizgavanje CSV-a

Ranjiva verzija: 2.4 i stariji

Broj pogođenih web lokacija: 20 000+

„Otkrivena je ranjivost CSV ubrizgavanja u WooCommerce - Store Exporter v 2.3.1. Omogućuje korisniku s povlasticama niske razine da ubrizga naredbu koja će biti uključena u izvezenu CSV datoteku, što dovodi do moguće izvršenja naredbe / koda. "

Pročitajte više o ranjivom dodatku na: https://fortiguard.com/zeroday/FG-VD-20-001

Authentication Bypass in Backup and Staging by WP Time Capsule

Ranjivost: Zaobilazni identitet

Ranjiva verzija: 1.21.16 i stariji

Broj pogođenih web lokacija: 20 000+

Pročitajte više o ranjivom dodatku na: https://www.webarxsecurity.com/vulnerability-infinitewp-client-wp-time-capsule/

Authentication Bypass in InfiniteWP Client Plugin

Ranjivost: Zaobilazni identitet

Ranjiva verzija: 1.9.4.5 i stariji

Broj pogođenih web lokacija: 300 000+

Pročitajte više o ranjivom dodatku na: https://www.webarxsecurity.com/vulnerability-infinitewp-client-wp-time-capsule/

Multiple Vulnerabilities Patched in Minimal Coming Soon & Maintenance Mode – Coming Soon Page Plugin

Ranjivost: CSRF za pohranjeni XSS i postavljanje promjena

Ranjiva verzija: 2.15 i stariji

Broj pogođenih web lokacija: 80 000+

Ranjivost: nesigurna dopuštenja: omogućiti i onemogućiti način održavanja

Ranjiva verzija: 2.15 i stariji

Broj pogođenih web lokacija: 80 000+

Ranjivosti: nesigurna dopuštenja: postavke izvoza / promjena teme

Ranjiva verzija: 2.15 i stariji

Broj pogođenih web lokacija: 80 000+

Pročitajte više o ranjivom dodatku na: https://www.wordfence.com/blog/2020/01/multiple-vulnerabilities-patched-in-minimal-coming-soon-maintenance-mode-coming-soon-page-plugin/

Multiple CSRF & XSS in Ultimate Auction Plugin

Ranjivosti: Višestruki CSRF i XSS

Ranjiva verzija: 4.0.6 i stariji

Broj pogođenih web lokacija: 3 000+

Pročitajte više o ranjivom dodatku na: https://plugins.trac.wordpress.org/changeset/2214112

Authenticated Code Injection in ElegantThemes (Divi, Extra, Divi-Builder)

Vrsta ranjivosti: Autentično ubrizgavanje koda

Ranjiva verzija: 4.0.10 i stariji

Broj pogođenih mjesta: N / A

Otkrivanje ranjivosti ubrizgavanja koda otkriveno je tijekom rutinske revizije koda koja bi mogla omogućiti da autori prijavljeni, autori i urednici prijavljeni izvršavaju mali skup PHP funkcija.

Pogođeni:

- Divi verzija 3.23 i novija

- Extra 2,23 i više

- Divi Builder, verzija 2.23 i novija.

Verzije proizvoda 4.0.10 uključuju sigurnosnu zakrpu.

Pročitajte više o ranjivom dodatku na: https://us7.campaign-archive.com/?u=9ae7aa91c578052b052b864d6&id=e3532c8cb1

CSRF to XSS in WooCommerce Conversion Tracking Plugin

Ranjivost: CSRF na XSS

Ranjiva verzija: 2.0.5 i stariji

Broj pogođenih web lokacija: 20 000+

Pročitajte više o ranjivom dodatku na: https://plugins.trac.wordpress.org/changeset/2220764

Post Submission Spoofing & Stored XSS in Postie Plugin

Ranjivost: Izdvajanje spoofinga i pohranjenih XSS

Ranjiva verzija: 1.9.40 i stariji

Broj pogođenih web lokacija: 20 000+

Dodatak Postie za WordPress omogućava samo objavljivanje članaka koje su poslali ovlašteni korisnici putem liste pošte koja je registrirana u postavkama dodatka.

Multiple Vulnerabilities in Import Users From CSV with Meta

Ranjivost: Neovlašteni izvoz autentificiranih korisnika

Ranjiva verzija: 1.15

Broj pogođenih web lokacija: 30 000+

Čini se da utječe samo inačica 1.15, jer je funkcionalnost izvoza nova značajka koju je ona uvela.

Unauthenticated Reflected XSS in Ultimate FAQ Plugin

Ranjivost: Neovjereno odraženi XSS

Ranjiva verzija: 1.8.30 i stariji

Broj pogođenih web lokacija: 40 000+

Arbitrary API Key update via CSRF in WP Simple Spreadsheet Fetcher For Google Plugin

Ranjivost: proizvoljno ažuriranje ključa API-ja putem CSRF-a

Ranjiva inačica: 0.3.7 i stariji

Broj pogođenih mjesta: oko 10

Nedostatak provjere zahtjeva za krivotvorenje web stranica (CSRF) na stranici postavki dodatka mogao bi omogućiti CSRF napadima postavljanje proizvoljnog API ključa.

Pročitajte više o ranjivom dodatku na: https://plugins.trac.wordpress.org/changeset/2222358

Zaključak: Uvijek ažurirajte ranjive dodatke

WordPressa web stranice svakodnevno se hakiraju. Neke statistike kažu da se oko 30 000 web stranica zarazi s nekom vrstom zlonamjernog softvera dnevno. Svaka javna web stranica resurs je dostupan na Internetu i stoga je ista cilj za hakiranje.

Važno je razumjeti da čim web stranica postane dostupna javnosti, **ona odmah postaje meta.**

Može proći samo nekoliko dana od otkrivene ranjivosti dodatka do pune akcije napada. Napadi u ovoj prirodi gotovo su uvijek automatizirani.

Uvijek, ali uvijek ažurirajte svoje dodatke kako ne biste imali ranjive dodatke na svojoj web stranici. Ako je moguće, omogućite automatsko ažuriranje.

Ako koristite neki od spomenutih dodataka, morate ga ažurirati što je prije moguće kako biste bili sigurni da sigurnosne ranjivosti dodataka WordPress neće utjecati na vaše web stranice.