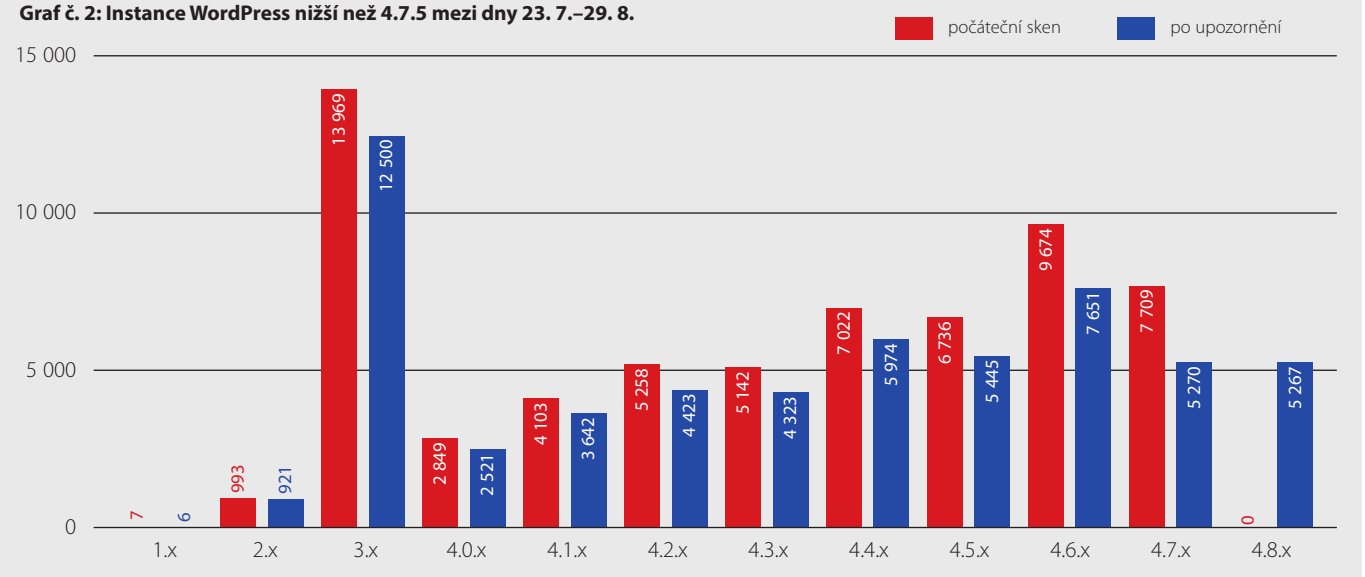
Graf č. 2: Instance WordPress nižší než 4.7.5 mezi dny 23. 7.–29. 8.



Tabulka: Vývoj zranitelností v jednotlivých verzích WordPressu

Verze CMS WordPress	Počáteční sken	Po upozornění
4.5.1	61	45
4.5.2	255	219
4.5.3	447	364
4.5.4	82	75
4.5.5	8	8
4.5.6	35	35
4.5.7	12	11
4.5.8	12	9
4.5.9	5 738	4 608
4.6	174	132
4.6.1	927	759
4.6.2	51	38
4.6.3	53	45
4.6.4	38	28
4.6.5	28	19
4.6.6	8 376	6 630
4.7	5 279	3 423
4.7.1	153	124
4.7.2	973	752
4.7.3	885	618
4.7.4	419	276
4.7.5	N/A	75
4.7.6	N/A	2

Zde je důležité zmínit, že testy se uskutečnily pouze na doménách druhého řádu; tedy například dobradomena.cz.

Zmíněná e-mailová zpráva přitom byla pouhým upozorněním informačního charakteru, takže držitelé domén, kteří o daném riziku věděli nebo nápravu již vykonali, mohli danou zprávu ignorovat.

Skript na zjišťování verzí z redakčních systémů se spouštěl z IP adresy 217.31.192.50, která je dedikovaná právě na výzkumné aktivity sdružení CSIRT.CZ, přičemž se důsledně používala HTTP hlavička User-Agent s hodnotou *csirt.cz CMS seeker*, aby příslušní webmasteři mohli činnost výzkumníků snadno identifikovat.

Co testování přineslo?

Nejlépe jsou výsledky testů vidět na publikovaných grafech. Aby se zachovala přehlednost, výsledky se sjednotily podle jednotlivých tzv. major (hlavních) verzí jak u Joomly (graf č. 1), tak u WordPressu (graf č. 2).

Aby bylo možné výsledky první vlny skenování ze 23. července s čím porovnat, test se na konci srpna zopakoval.

Z nových výsledků je například zřejmé, že ke změně došlo celkem u 10 514 domén. Není samozřejmě možné vyhodnotit, kolik webů přešlo na vyšší verze v důsledku zmíněného upozornění, protože prostě mohlo jít o přirozený, pravidelný přechod na novou verzi, ale i tak je to pozitivní úkaz.

Poměrně velká část e-mailových upozornění navíc nemohla být doručená v důsledku špatně uvedené e-mailové adresy držitele domény v registru.

I to je důvod, proč sdružení CZ.NIC dělá různé akce na udržování aktuálních kontaktních údajů u domén. Právě na tyto kontakty se totiž zasílají také informační e-maily o expiraci domény.

Pokud se shrne reakce na zasílané e-maily, byly spíše pozitivní a velice často obsahovaly informaci o tom, že aktualizace již proběhla, nebo dotazy, jak vlastně takovou aktualizaci udělat. Ukázalo se totiž, že mnoho uživatelů neví, jak daný redakční systém aktualizovat.

Pro doplnění je dobré ještě uvést, jak vypadal mezi červencem a srpnem vývoj v jednotlivých verzích poslední hlavní verze WordPressu, viz tabulku.

[Mnoho uživatelů neví, jak daný redakční systém aktualizovat.]

A výsledek?

Přestože výzkumníci CSIRT.CZ po testování obdrželi také několik negativních reakcí, pozitivní odezva převažovala. Díky těmto kladným reakcím a s ohledem na výsledky opakovaného testu považují experti zmíněného národního týmu CSIRT.CZ tuto akci za úspěšnou. Cílem akcí tohoto typu jsou pro ně snaha o nápravu současného stavu a osvěta.

Nadále nezabezpečené systémy jsou samozřejmě problémem pro ty, kteří je využívají pro provoz svých internetových služeb. Mnohem větší potíže ale představují pro běžné internetové uživatele, tedy internetové laiky. ■

Autorka pracuje jako bezpečnostní analytička sdružení CZ.NIC.