Mesačný prehľad kritických zraniteľností
Marec 2019

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci marec 6 kritických zraniteľností. Jednou z nich je zraniteľnosť CVE-2019-0784, ktorá umožňuje vzdialené vykonávanie kódu. Vzniká pri nesprávnom pristupovaní Active Data objektov (ADO) ku objektom v pamäti. Ak útočník zneužije túto zraniteľnosť, získa rovnaké práva ako prihlásený používateľ. Ak je teda prihlásený administrátor, útočník získa práva administrátora a tak aj kontrolu nad celým systémom. Z hľadiska webového útoku musí útočník hostiť webstránku, ktorej obsah je prispôsobený na využitie tejto zraniteľnosti cez Interner Explorer. Potom musí presvedčiť používateľa, aby navštívil danú webovú stránku. Takisto môže útočník vložiť ovládací prvok ActiveX označený ako „bezpečný pre inicializáciu“ do aplikácie alebo dokumentu Microsoft Office, ktorý je hostiteľom nástroja na vykresľovanie IE. Druhou zraniteľnosťou je CVE-2019-0756. Vzniká, ak Microsoft XML Core Services (MSXML) spracuváva vstupy používateľa. Po zneužití zraniteľnosti môže útočník vzdialene vykonávať škodlivý kód a získava kontrolu nad systémom používateľa. Na zneužitie môže použiť upravenú webovú stránku, ktorá vyvolá MSXML cez webový prehliadač. Útočník musí presvedčiť používateľa, aby navštívil danú webstránku napríklad cez link v emaile.
Ďalšie kritické zraniteľnosti CVE-2019-0726, CVE-2019-0698, CVE-2019-0697 sa týkajú DHCP servera. Útočník môže poškodiť pamäť, ak pošle špeciálne upravené DHCP odpovede klientovi. Po zneužití dokáže vykonávať škodlivý kód na zariadení klienta.
Bola opravená aj kritická zraniteľnosť CVE-2019-0603 vo Windows Deployment Services TFTP serveri. Vzniká pri pristupovaní ku objektom v pamäti týmto serverom. Na zneužitie zraniteľnosti je potrebné vytvoriť špeciálnu požiadavku, ktorá spôsobí, že Windows spustí ľubovoľný kód so zvýšenými oprávneniami. Útočníkovi umožňuje vykonávať ľubovoľný kód na zraniteľnom systéme.

Opravených bolo aj 8 závažných zraniteľností. Zraniteľnosť CVE-2019-0759 týkajúca sa softvéru Windows Print Spooler, zraniteľnosti CVE-2019-0755 a CVE-2019-0702 a ďalšie v jadre Windows umožňujúce útočníkovi získať informácie a neskôr kompromitovať používateľa. Zraniteľnosti CVE-2019-0704, CVE-2019-0703 týkajúce sa servera Windows SMB. CVE-2019-0776 zraniteľnosť v komponente win32k a CVE-2019-0774, CVE-2019-0614 v komponente Windows GDI.

Zraniteľné systémy:

Windows 10 for 32-bit Systems
Windows 10 for x64-based Systems
Windows 10 Version 1607 for 32-bit Systems
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 1703 for 32-bit Systems
Windows 10 Version 1703 for x64-based Systems
Windows 10 Version 1709 for 32-bit Systems

Windows 10 Version 1709 for 64-based Systems
Windows 10 Version 1709 for ARM64-based Systems
Windows 10 Version 1803 for 32-bit Systems
Windows 10 Version 1803 for ARM64-based Systems
Windows 10 Version 1803 for x64-based Systems
Windows 10 Version 1809 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows 10 Version 1809 for x64-based Systems
Windows 7 for 32-bit Systems Service Pack 1
Windows 7 for x64-based Systems Service Pack 1
Windows 8.1 for 32-bit systems
Windows 8.1 for x64-based systems
Windows RT 8.1
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows Server 2008 for x64-based Systems Service Pack 2
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Server 2012
Windows Server 2012 (Server Core installation)
Windows Server 2012 R2
Windows Server 2012 R2 (Server Core installation)
Windows Server 2016
Windows Server 2016 (Server Core installation)
Windows Server 2019
Windows Server 2019 (Server Core installation)
Windows Server, version 1709 (Server Core Installation)
Windows Server, version 1803 (Server Core Installation)

Odporúčania:

Odporúčame aplikovať aktualizácie publikované prostredníctvom služby Windows Update. Číslo aktualizácie pre konkrétny systém možno vyhľadať na prvom z nižšie uvedených odkazov vložením identifikátora zraniteľnosti do vyhľadávania.

Zdroje:

https://portal.msrc.microsoft.com/en-us/security-guidance
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0784
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0756
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0726
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0698
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0697

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0603
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0755
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0759
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0702
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0703
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0704
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0776
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0774
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0614

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft opravila tento mesiac dve závažné zraniteľnosti. Prvá zraniteľnosť CVE-2019-0748 vzniká, ak Microsoft Office Access Connectivity Engine (MOACE) nevhodne pristupuje ku objektom v pamäti. Útočníkovi umožňuje vzdialene vykonávať kód na zraniteľnom systéme. Útočník môže zneužiť zraniteľnosť, ak naláka obeť, aby otvorila infikovaný súbor. Cross-site skriptovacia (XSS) zraniteľnosť CVE-2019-0778 vzniká, ak Microsoft SharePoint server nedostatočne ošetrí špeciálne upravené webové požiadavky na zraniteľný server SharePoint. Útočník zneužije zraniteľnosť, ak pošle danú špeciálnu požiadavku. Potom môže vykonávať cross-site skriptovacie útoky, ktoré mu umožnia prečítať si obsah, na ktorý nemá oprávnenia, môže v mene napadnutého používateľa vykonávať akcie v SharePoint sieti, ako napríklad zmeniť oprávnenia, vymazať dáta alebo vložiť škodlivý obsah do prehliadača používateľa.

Zraniteľné systémy:

Microsoft Office 2010 Service Pack 2 (64-bit editions)
Microsoft Office 2010 Service Pack 2 (32-bit editions)
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Foundation 2013 Service Pack 1

Odporúčania:

Odporúčame aplikovať aktualizácie publikované prostredníctvom služby Windows Update. Číslo aktualizácie pre konkrétny systém možno vyhľadať na prvom z nižšie uvedených odkazov vložením identifikátora zraniteľnosti do vyhľadávania.

Zdroje:

https://portal.msrc.microsoft.com/en-us/security-guidance
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0748
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0778

3. Internetové prehliadače

Microsoft Internet Explorer

Aktualizácia od spoločnosti Microsoft opravuje 5 kritických zraniteľností. CVE-2019-0763, CVE-2019-0680, CVE-2019-0609 zraniteľnosť je spôsobená nevhodným pristupovaním systému ku objektom v pamäti. Na zneužitie zraniteľnosti útočník môže hostiť webstránku, ktorej obsah je prispôsobený na využitie tejto zraniteľnosti cez Interner Explorer. Potom sa mu musí podariť presvedčiť používateľa, aby otvoril škodlivú webstránku. Útočník môže takisto využiť kompromitované webové stránky alebo webové stránky, ktoré prijímajú alebo hostia obsah alebo reklamy poskytované používateľom na pridanie infikovaného súboru. Naviac, môže útočník vložiť ovládací prvok ActiveX označený ako „bezpečný pre inicializáciu“ do aplikácie alebo dokumentu Microsoft Office, ktorý je hostiteľom nástroja na vykresľovanie IE. Niekedy sa od používateľa očakáva aktívny prístup (kliknutie na odkaz,..). Zneužitie tejto zraniteľnosti umožňuje vzdialené vykonávanie kódu. Útočník získava rovnaké práva ako prihlásený používateľ. Ak je prihlásený administrátor, útočník získa práva administrátora a získa kontrolu nad celým systémom.

Ďalšia zraniteľnosť CVE-2019-0666 a CVE-2019-0667 umožňuje vzdialené vykonávanie kódu, ak skriptovací nástroj (VBScript engine) nevhodne pristupuje ku objektom v pamäti. Útočník po zneužití zraniteľnosti získava rovnaké práva ako momentálne prihlásený používateľ. Ak je teda prihlásený administrátor, útočník môže získať kontrolu nad celým systémom. Na zneužitie tejto zraniteľnosti je potrebné hostiť webstránku, ktorej obsah je prispôsobený na využitie danej zraniteľnosti cez Internet Explorer. Potom musí presvedčiť používateľa, aby navštívil danú stránku. Útočník môže takisto využiť kompromitované webové stránky alebo webové stránky, ktoré prijímajú alebo hostia obsah alebo reklamy poskytované používateľom na vloženie infikovaného obsahu. Naviac, môže útočník vložiť ovládací prvok ActiveX označený ako „bezpečný pre inicializáciu“ do aplikácie alebo dokumentu Microsoft Office, ktorý je hostiteľom nástroja na vykresľovanie IE.

Zraniteľné systémy:

Microsoft Internet Explorer verzie 10

Microsoft Internet Explorer verzie 11

Odporúčania:

Odporúčame aplikovať aktualizácie publikované prostredníctvom služby Windows Update. Číslo aktualizácie pre konkrétny systém možno vyhľadať na prvom z nižšie uvedených odkazov vložením identifikátora zraniteľnosti do vyhľadávania.

Zdroje:

https://portal.msrc.microsoft.com/en-us/security-guidance

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0763

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0666

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0667

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0680

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0609

Microsoft Edge

Spoločnosť Microsoft opravila tento mesiac 7 kritických zraniteľností. Zraniteľnosť CVE-2019-0773, CVE-2019-0771, CVE-2019-0770, CVE-2019-0769, CVE-2019-0639, CVE-2019-0609, CVE-2019-0592 umožňuje vzdialené vykonávanie kódu, ak skriptovací nástroj nevhodne pristupuje ku objektom v pamäti. Na zneužitie tejto zraniteľnosti je potrebné hostiť webstránku, ktorej obsah je prispôsobený na využitie danej zraniteľnosti cez Microsoft Edge. Potom musí presvedčiť používateľa, aby navštívil danú stránku. Útočník môže takisto využiť kompromitované webové stránky alebo webové stránky, ktoré prijímajú alebo hostia obsah alebo reklamy poskytované používateľom. Útočník tak získava rovnaké práva ako momentálne prihlásený používateľ. Ak je teda prihlásený administrátor, útočník môže získať kontrolu nad celým systémom.

Zraniteľné systémy:

Microsoft Edge v systémoch Windows 10 verzie 1809 v 32-bitových, 64-bitových verziách aj ARM64 verzii
Microsoft Edge v systémoch Windows Server 2019
Microsoft Edge v systémoch Windows Server 2016
ChakraCore
Windows 10 Version 1703 for 32-bit Systems, x64-based Systems
Windows 10 Version 1709 for 32-bit Systems, x64-based Systems, ARM64-based Systems
Windows 10 Version 1803 for 32-bit Systems, x64-based Systems, ARM64-based Systems
Windows 10 for 32-bit Systems, x64-based Systems
Windows 10 Version 1607 for 32-bit Systems
Windows 10 Version 1607 for x64-based Systems

Odporúčania:

Odporúčame aplikovať aktualizácie publikované prostredníctvom služby Windows Update. Číslo aktualizácie pre konkrétny systém možno vyhľadať na prvom z nižšie uvedených odkazov vložením identifikátora zraniteľnosti do vyhľadávania.

Zdroje:

https://portal.msrc.microsoft.com/en-us/security-guidance
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0773
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0771
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0770
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0769
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0639

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0609
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0592

Mozilla Firefox

Spoločnosť Mozilla opravila tento mesiac 7 kritických zraniteľností. Prvou opravenou zraniteľnosťou je CVE-2019-9813, spôsobená nesprávnym spracovaným proto_mutations. Môže viesť ku zámene v IonMonkey JIT kóde a neskôr ku prepisovaniu a čítaniu z pamäte. Druhou opravenou zraniteľnosťou je CVE-2019-9810. Vzniká ak má IonMonkey JIT kompilátor nesprávne informácie a môže viesť ku nekontrolovaniu hraníc a následného pretečenia vyrovnávacej pamäte. Treťou opravenou zraniteľnosťou je CVE-2019-9790. Zraniteľnosť „use-after-free“ (použitie odalokovaného miesta v pamäti) môže nastať, keď ukazovateľ na DOM element získa na stránke používaný JavaScript, a kým ho používa je element odstránený. Štvrtou opravenou zraniteľnosťou je CVE-2019-9791. Ak systém umožní kompiláciu funkcií, pri ktorých môže dôjsť ku zámene nejakých objektov, kým prechádzajú kompiláciou IonMonkey JIT kompilátora a ak je zadaný konštruktor cez on-stack replacement, vzniká daná zraniteľnosť a je možné čítať a prepisovať objekty. Piatou opravenou zraniteľnosťou je CVE-2019-9792, ktorá vzniká ak dôjde ku strate hodnoty počas bežania bailoutu. Pri zneužití tejto zraniteľnosti je daná hodnota využitá JavaScriptom na poškodenie pamäti. Opravené boli aj zraniteľnosti CVE-2019-9789 a CVE-2019-9788, ktoré umožňujú poškodenie pamäte a vykonávanie škodlivého súboru.
Opravených bolo aj 7 závažných zraniteľností, umožňujúcich čítanie z pamäti, man-in-the-middle útok, vykonanie spustiteľných súborov a ďalšie.

Zraniteľné systémy:

Mozilla Firefox verzie staršie ako 66.0.1
Mozilla Firefox ESR verzie staršie ako 60.6.1

Odporúčania:

Vzhľadom na počet kritických zraniteľností odporúčame bezodkladne aktualizovať na najnovšiu verziu.

Zdroje:

https://www.mozilla.org/en-US/security/advisories/

https://www.mozilla.org/en-US/security/advisories/mfsa2019-10/

https://www.mozilla.org/en-US/security/advisories/mfsa2019-07/

Google Chrome

Spoločnosť Google opravila viac ako 60 zraniteľností v mesiaci marec. Z nich bolo 6 závažných. Zraniteľnosti CVE-2019-5787, CVE-2019-5787, CVE-2019-5787 sú typu „use-after-free“ (použitie odalokovaného miesta v pamäti), CVE-2019-5790 je spôsobená pretečením

vyrovnávacej pamäte typu halda vo V8, CVE-2019-5791 vzniká pri určitých nejasnostiach vo V8 a CVE-2019-5792 celočíselným pretečením v PDFium.

Zraniteľné systémy:
Google Chrome verzie staršie ako 73.0.3683.88

Odporúčania:

Vzhľadom na veľký počet opravených zraniteľností odporúčame aktualizáciu na najnovšiu verziu.

Zdroje:
https://chromereleases.googleblog.com/2019
https://chromereleases.googleblog.com/2019/03/stable-channel-update-for-chrome-os_25.html
https://chromereleases.googleblog.com/2019/03/stable-channel-update-for-desktop_12.html

4. Adobe Flash Player, Acrobat a Reader

Tento mesiac neboli opravené žiadne zraniteľnosti v Adobe Flash Player, Acrobat a Reader.

Zdroje:

https://helpx.adobe.com/security.html

5. Frameworky

Microsoft .NET Framework

Tento mesiac spoločnosť Microsoft nevydala žiadne aktualizácie opravujúce zraniteľnosti.

Zdroje:
https://portal.msrc.microsoft.com/en-us/security-guidance

Oracle Java

Spoločnosť Oracle nevydala v mesiaci marec žiadne aktualizácie platformy Java. Najbližšia veľká sada aktualizácií je naplánovaná na 16. apríl 2019.

Zdroje:
https://www.oracle.com/technetwork/topics/security/alerts-086861.html

6. Iné závažné zraniteľnosti

Aktívne zneužívaná 19-ročná kritická zraniteľnosť vo WinRARe

V aplikácii na kompresiu dát WinRAR bola opravená kritická zraniteľnosť CVE-2018-20250 umožňujúca útočníkom vzdialene vykonávať kód. Zraniteľné sú všetky verzie vydané za posledných 19 rokov pred opravnou aktualizáciou 5.70 beta 1. V prvom týždni po zverejnení zraniteľnosti bolo zaznamenaných vyše 100 rôznych kampaní, v ktorých bola zneužívaná. Nakoľko WinRAR nepodporuje automatické aktualizácie, používatelia si musia novú verziu nainštalovať manuálne.

Dôsledky:

- Vykonávanie škodlivého kódu
- Prevzatie kontroly nad systémom používateľa

Opis činnosti:

Bezpečnostný výskumník Nadav Grossman zo spoločnosti Check Point objavil kritickú zraniteľnosť v obľúbenej aplikácii na kompresiu dát WinRAR, s ktorou pracuje pol miliardy používateľov. Ovplyvňuje všetky predchádzajúce verzie pred opravnou aktualizáciou 5.70 beta 1, vydané počas 19 rokov. Zraniteľnosť CVE-2018-20250 je aktívne zneužívaná a umožňuje traverzovanie absolútnej cesty, čo môže viesť ku vzdialenému vykonávaniu kódu a prevzatiu plnej kontroly nad zariadením obete. Nachádza sa v UNACEV2.DLL knižnici a útočník vďaka nej dokáže extrahovať komprimovaný spustiteľný súbor z archívu ACE do spúšťacieho priečinka Windows Startup. Škodlivý súbor sa automaticky spustí pri nasledujúcom reštartovaní operačného systému. Jediné čo musia útočníci vykonať, je presvedčiť používateľa, aby tento škodlivý súbor používatelia otvorili pomocou zraniteľnej verzie programu WinRAR. Na to začali hneď po vydaní funkčnej ukážky zneužiteľnosti zraniteľnosti využívať spamovú kampaň šíriacu malvér.

Výskumníci zo spoločnosti McAfee informovali o vyše 100 rôznych exploitoch, využitých v prvý týždeň po zverejnení zraniteľnosti. Jedným príkladom je archív Ariana_Grande-thank_u,_next(2019)_[320].rar, ktorý okrem extrahovania neškodných MP3 súborov do počítača používateľa extrahuje škodlivý .EXE súbor do zložky Startup, navrhnutý na infikovanie systému. Pritom obchádza kontrolu User Access Control (UAC), teda používateľovi sa nezobrazí žiadna výstraha a pri ďalšom reštartovaní sa malware vykoná.

Nakoľko zdrojový kód knižnice UNACEV2.DLL sa stratil, oprava zraniteľnosti spočívala v odstránení podpory pre ACE archívy z WinRAR. V prípade potreby podpory týchto archívov je však riešenie dostupné v podobe mikrozáplaty od spoločnosti ACROS Security cez platformu

0Patch. V prípade pokusu o rozbalenie infikovaného archívu tak program používateľovi zobrazí niekoľko varovaní.

Zraniteľné systémy

WinRAR, všetky verzie pred 5.70 beta 1
Systémy používajúce archív ACE

Závažnosť zraniteľnosti

Vysoká

Možné škody

Vzdialené vykonávanie kódu

Odporúčania

Vzhľadom na aktívne zneužívanie sa odporúča aktualizovať WinRAR aspoň na verziu 5.70 beta 1 a vyhýbať sa otváraniu súborov z nedôveryhodných zdrojov.

Odkazy

https://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=237
https://www.bleepingcomputer.com/news/security/over-100-exploits-found-for-19-year-old-winrar-rce-bug/
https://www.bleepingcomputer.com/news/security/19-year-old-winrar-rce-vulnerability-gets-micropatch-which-keeps-ace-support/
https://thehackernews.com/2019/03/winrar-hacking-malware.html

Kritická zraniteľnosť WordPress umožňuje ľahko ovládnuť webstránku cez komentáre

Zraniteľnosť v Content Management Software (CMS) môže viesť ku vzdialenému vykonávaniu kódu. Zraniteľnosť vzniká pri chybných cross-site požiadavkách (CSRF) v časti pre komentáre v programe WordPress. Táto časť programu je jednou zo základných súčastí, ktorá je štandardne povolená a ovplyvňuje všetky inštalácie programu WordPress pred verziou 5.1.1. Daná zraniteľnosť dokonca umožňuje neautentifikovanému vzdialenému útočníkovi, aby kompromitoval systém a vzdialene vykonával kód na zraniteľných webových stránkach.

Dôsledky

- Vzdialené vykonávanie kódu

- Kompromitácia systému

Opis činnosti

Výskumník Simon Scannell zo spoločnosti RIPS Technologies objavil novú chybu v CMS WordPress. Útočník ju môže zneužiť tak, že presvedčí administrátora zraniteľnej webstránky, aby navštívil jeho škodlivú stránku. Pri demonštrácii novej zraniteľnosti poukázal na problémy, ktoré umožňujú využívať danú zraniteľnosť:

- WordPress nepoužíva CSRF overenie, keď používateľ pridáva nový komentár, a teda útočník môže pridať komentár v mene administrátora.
- Komentáre pridané administrátorom nie sú kontrolované a môžu obsahovať škodlivé HTML, alebo SCRIPT značky (tagy).
- WordPress nie je chránený X-Frame-Options hlavičkou, čo umožňuje útočníkovi otvoriť cielenú stránku s pomocou ukrytého iFrame z webovej stránky ním ovládanej.

Kombináciou týchto problémov môže útočník nepozorovane vložiť škodlivý XSS kód zo svojej stránky do cieľovej webovej stránky tým, že administrátor-obeť navštívi túto škodlivú webovú stránku. Podľa Scannella, útočník dokonca môže získať úplnú kontrolu nad cielenou stránkou, ak vloží vzdialene XSS kód, ktorý upraví šablónu WordPressu priamo, tak aby vložil PHP zadné vrátka. A to bez vedomia administrátora.

Zraniteľné systémy

WordPress verzie staršie ako 5.1.1

Závažnosť zraniteľnosti

Vysoká

Možné škody

Cross-site scripting (XSS) Vzdialené vykonávanie kódu

Odporúčania

Bezodkladne aktualizovať na verziu 5.1.1, ak to program neurobil automaticky.

Odkazy

https://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=236
https://thehackernews.com/2019/03/hack-wordpress-websites.html
https://blog.ripstech.com/2019/wordpress-csrf-to-rce/
https://securityaffairs.co/wordpress/82382/hacking/wordpress-csrf-hack.html
https://www.bleepingcomputer.com/news/security/wordpress-511-fixes-xss-vulnerability-leading-to-website-takeovers/

Kritická zraniteľnosť v balíkoch Pacman

Bola nájdená kritická zraniteľnosť CVE-2019-9686 v manažéri softvérových balíčkov Pacman. Zraniteľnosť umožňuje vykonávanie škodlivého kódu ak si používateľ inštaluje balík zo špeciálnej URL adresy. Ide o útok man-in-the-middle.

Dôsledky

Vzdialené vykonávanie škodlivého kódu

Opis činnosti

CVE-2019-9686
Pacman verzie nižšej ako 5.1.3 umožňuje traverzovanie medzi priečinkami pri inštalovaní balíka cez URL adresu príkazom “pacman –U“.

Zraniteľné systémy

Linux manažér balíčkov Pacman, verzie staršie ako 5.1.3-1

Závažnosť zraniteľnosti

Vysoká

Možné škody

Vzdialené vykonávanie kódu

Odporúčania

Bezodkladne aktualizovať Pacman na verziu 5.1.3-1

Odkazy

https://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=235
https://security.archlinux.org/ASA-201903-7
https://nvd.nist.gov/vuln/detail/CVE-2019-9686
https://security-tracker.debian.org/tracker/CVE-2019-9686

Aktívne zneužívaná zero-day zraniteľnosť v prehliadači Google Chrome

Kritická zraniteľnosť v prehliadači Google Chrome typu "Use after free" (použitie odalokovaného miesta v pamäti) umožňuje vzdialene vykonávať kód v systéme obete a prevziať tak kontrolu nad jej zariadením. Zraniteľnosť je aktívne zneužívaná a spoločnosť Google na ňu nedávno vydala opravu. Odporúča sa bezodkladne aktualizovať prehliadač Chrome.

Dôsledky

- Zvýšenie práv a únik zo Sandboxu prehliadača Chrome

- Vzdialené vykonávanie kódu
- Prevzatie kontroly nad zariadením
- Vyvolanie DoS podmienok

Opis činnosti

CVE-2019-5786

Spoločnosť Google opravila kritickú zero-day chybu v prehliadači Google Chrome po tom, ako ju objavil výskumník Clement Lecigne z tímu Google Threat Analysis Group. Zraniteľnosť je aktívne zneužívaná.

Zraniteľnosť sa nachádza v API komponente FileReader, používanom na asynchrónne čítanie obsahu súborov na disku, alebo dát z medzipamäte. Umožňuje použiť odalokované miesto v pamäti, čo môže viesť k zvýšeniu práv útočníka a možnosti vzdialene vykonávať ľubovoľný kód v systéme obete s právami práve prihláseného používateľa. Môže nastať tiež pád aplikácie a narušenie dostupnosti systému.

Pre zneužitie zraniteľnosti stačí, keď útočník presvedčí obeť, aby navštívila škodlivú webstránku, prípadne ju na svoju webstránku presmeruje.

Zraniteľné systémy

Google Chrome, verzie staršie ako 72.0.3626.121

Závažnosť zraniteľnosti

Stredná

Možné škody

Narušenie dostupnosti systému (Dos)
Vzdialené vykonávanie kódu

Odporúčania

Bezodkladná aktualizácia Google Chrome aspoň na verziu 72.0.3626.121

Odkazy

https://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=234
https://www.bleepingcomputer.com/news/security/google-chrome-update-patches-zero-day-actively-exploited-in-the-wild/
https://thehackernews.com/2019/03/update-google-chrome-hack.html
https://www.tenable.com/blog/use-after-free-vulnerability-in-google-chrome-exploited-in-the-wild-cve-2019-5786