Mesačný prehľad kritických zraniteľností
Február 2019

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft zverejnila tento mesiac opravu 3 kritických zraniteľností. Dve z nich, CVE-2019-0662 a CVE-2019-0618, umožňujú vzdialené vykonávanie kódu. Týkajú sa komponentu GDI a vznikajú pri sprístupňovaní obsahu v pamäti daným komponentom. Ich zneužitím získa útočník kontrolu nad zraniteľným systémom. Napadnúť používateľa môže útočník rôznymi spôsobmi, napríklad ak presvedčí používateľa, aby otvoril súbor, ktorý je infikovaný.
Tretia kritická zraniteľnosť CVE-2019-0626 sa týka DHCP servera. Útočník môže poškodiť pamäť, ak pošle špeciálne upravený paket na DHCP server. Spoločnosť opravila aj závažné zraniteľnosti ako CVE-2019-0636 spôsobenú nesprávnym sprístupnením informácií o súboroch. Zneužitím tejto zraniteľnosti dokáže útočník prečítať obsah súborov zapísaných na disku, avšak, aby ju dokázal zneužiť, musel by sa prihlásiť do daného systému a spustiť špeciálne upravenú aplikáciu. Zraniteľnosť CVE-2019-0635 nastáva, keď sú nesprávne spracované vstupy od používateľa hosťovského systému pomocou Windows Hyper-V na hostiteľovi. Zneužiť túto zraniteľnosť je možné tak, že útočník spustí špeciálne pripravenú aplikáciu na hosťovskom operačnom systéme a tým spôsobí únik informácií z pamäte hostiteľa. Útočník má teda možnosť pristúpiť k týmto informáciám. Opravené boli aj zraniteľnosti CVE-2019-0600, CVE-2019-0601 pre komponent Human Interface Devices (HID). Zraniteľnosť umožňujúca únik informácií je spôsobená nesprávnym pristupovaní ku objektom v pamäti. Útočník je schopný použiť uniknuté informácie na kompromitovanie počítača používateľa. Na zneužitie zraniteľnosti je potrebné získať oprávnenia umožňujúce spustenie infikovanej aplikácie. Príčiny vzniku a dôsledky sú rovnaké aj pri zraniteľnostiach CVE-2019-0621, ktorá je závažná a CVE-2019-0661. Na zneužitie zraniteľností je potrebné, aby sa páchateľ prihlásil do daného systému a spustil špeciálne upravenú aplikáciu. Tieto zraniteľnosti sa týkajú jadra operačného systému Windows. Zraniteľnosti CVE-2019-0602, CVE-2019-0615, CVE-2019-0616, CVE-2019-0619, CVE-2019-0660, CVE-2019-0664 týkajúce sa komponentu GDI boli taktiež opravené. Zraniteľnosti umožňujúce únik informácií sú spôsobené nesprávnym sprístupnením obsahu v pamäti. Útočník je schopný použiť uniknuté informácie na kompromitovanie počítača používateľa. Útočník môže zneužiť tieto zraniteľnosti, ak presvedčí používateľa, aby otvoril infikovaný súbor alebo aby navštívil nedôveryhodnú stránku. Posledná závažná zraniteľnosť CVE-2019-0628, ktorá bola opravená sa týka komponentu win32k. Táto zraniteľnosť vzniká, ak daný komponent neposkytuje informácie jadru OS Windows vhodne. Páchateľ môže získať uniknuté informácie a potom kompromitovať systém používateľa. Avšak, musí sa prihlásiť do daného systému a spustiť infikovanú aplikáciu.

Zraniteľné systémy:

Windows 10 for 32-bit Systems
Windows 10 for x64-bit 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 x64-based Systems
Windows 10 Version 1709 for ARM64-based Systems
Windows 10 Version 1803 for 32-bit Systems
Windows 10 Version 1803 for x64-based Systems
Windows 10 Version 1803 for ARM64-based Systems
Windows 10 Version 1809 for 32-bit Systems
Windows 10 Version 1809 for x64-based Systems
Windows 10 Version 1809 for ARM64-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-2019-0635

https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0636

https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0600

https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0601
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0602
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0621
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0628
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0661
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0615
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0616
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0662
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0618
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0626

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft opravila tento mesiac 2 kritické zraniteľnosti. CVE-2019-0594 a CVE-2019-0604 umožňujú vzdialené vykonávanie kódu ak sa Microsoft SharePoint softvéru nepodarí skontrolovať zdrojové označenie balíka aplikácií. Ak útočník zneužije túto zraniteľnosť môže vykonávať škodlivý kód v aplikácii SharePoint. Zraniteľnosť CVE-2019-0540 umožňujúca obídenie bezpečnostných mechanizmov vzniká ak Microsoft Office nekontroluje URL adresy. Útočník môže používateľovi poslať špeciálne upravený súbor, pomocou ktorého dokáže od používateľa získať jeho prihlasovacie údaje pomocou phishingového útoku. Zverejnená bola aj oprava na závažnú zraniteľnosť CVE-2019-0669. Zraniteľnosť umožňujúca únik informácií je spôsobená nesprávnym sprístupnením obsahu v pamäti. Útočník je schopný použiť uniknuté informácie na kompromitovanie počítača používateľa alebo jeho dát. Na zneužitie tejto zraniteľnosti je potrebné, aby používateľ otvoril infikovaný súbor.

Zraniteľné systémy:

Microsoft Excel Viewer
Microsoft Office 2010 Service Pack 2 (32-bit editions)
Microsoft Office 2010 Service Pack 2 (64-bit editions)
Microsoft Office 2013 RT Service Pack 1
Microsoft Office 2013 Service Pack 1 (32-bit editions)
Microsoft Office 2013 Service Pack 1 (64-bit editions)
Microsoft Office 2016 (32-bit edition)
Microsoft Office 2016 (64-bit edition)
Microsoft Office 2019 for 32-bit editions
Microsoft Office 2019 for 64-bit editions
Microsoft Office Compatibility Pack Service Pack 3
Microsoft Office Word Viewer
Microsoft PowerPoint Viewer
Office 365 ProPlus for 32-bit Systems

Office 365 ProPlus for 64-bit Systems
Microsoft Excel 2010 Service Pack 2 (32-bit editions)
Microsoft Excel 2010 Service Pack 2 (64-bit editions)
Microsoft Excel 2013 RT Service Pack 1
Microsoft Excel 2013 Service Pack 1 (32-bit editions)
Microsoft Excel 2013 Service Pack 1 (32-bit editions)
Microsoft Excel 2016 (32-bit edition)
Microsoft Excel 2016 (64-bit edition)
Microsoft Office 2016 for Mac
Microsoft Office 2019 for Mac
Microsoft Office Compatibility Pack Service Pack 3

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-2019-0540

https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0669

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0594

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0604

3. Internetové prehliadače

Microsoft Internet Explorer

Aktualizácia od spoločnosti Microsoft opravuje 2 kritické zraniteľnosti CVE-2019-0676 a CVE-2019-0606, ktoré sú spôsobené nevhodným pristupovaním systému ku objektom v pamäti. Na zneužitie prvej zraniteľnosti sa musí útočníkovi podariť presvedčiť používateľa, aby otvoril škodlivú webstránku. Potom bude schopný zistiť prítomnosť súborov na disku. Bolo zaznamenané aktívne zneužívanie tejto zraniteľnosti. Na zneužitie druhej zraniteľnosti musí napríklad útočník hostiť webstránku, ktorej obsah je prispôsobený na využitie tejto zraniteľnosti. Pri všetkých spôsoboch sa od používateľa očakáva aktívny prístup (napr. otvorenie prílohy v maile). Zneužitie tejto zraniteľnosti umožňuje vzdialené vykonávanie kódu. Útočník získava rovnaké práva ako prihlásený používateľ. Ak je teda prihlásený administrátor, útočník získa práva administrátora a získa kontrolu nad celým systémom.

Zraniteľné systémy:

Microsoft Internet Explorer verzie 10
Microsoft Internet Explorer verzie 11

Odporúčania:

Vzhľadom na zaznamenané zneužívanie jednej zo zraniteľností sa odporúča aktualizovať systém na najnovšiu verziu.

Zdroje:

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

https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0676

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0606

Microsoft Edge

Spoločnosť Microsoft opravila tento mesiac 14 kritických zraniteľností. Opravila zraniteľnosti ako CVE-2019-0590, CVE-2019-0650, CVE-2019-0640, CVE-2019-0655 a ďalšie. Tieto zraniteľnosti umožňujú vzdialené vykonávanie kódu ak skriptovací nástroj nevhodne pristupuje ku objektom v pamäti. Na zneužitie týchto zraniteľností je potrebné hostiť webstránku, ktorej obsah je prispôsobený na využitie týchto zraniteľností. Potom musí útočník presvedčiť používateľa, aby navštívil danú stránku. Útočník tak získava rovnaké práva ako momentálne prihlásený používateľ. Ak je teda prihlásený administrátor, útočník môže získať kontrolu nad celým systémom. Zraniteľnosť CVE-2019-0643 vzniká pri spracovávaní dopytov. Útočník môže zistiť pôvod všetkých webstránok v zraniteľnom prehliadači. Bola opravená aj závažná zraniteľnosť CVE-2019-0648, pri ktorej dochádza ku úniku dát. Zraniteľnosť vzniká ak Chakra nevhodne sprístupňuje obsah v pamäti. Posledná závažná zraniteľnosť CVE-2019-0658 spôsobuje únik informácií ak skriptovací nástroj nevhodne pristupuje ku objektom v pamäti. Ak chce útočník zneužiť zraniteľnosť, musí hostiť webstránku, s vhodne upraveným obsahom. Útočník musí presvedčiť používateľa, aby navštívil danú stránku, napríklad kliknutím na link, ktorý ho na ňu presmeruje.

Opravené boli aj zraniteľnosti v Adobe Flash Player (viď nižšie).

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-2019-0643
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0648
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0658
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0590
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0640
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0655
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0650

Mozilla Firefox

Spoločnosť Mozilla tento mesiac opravila vo svojom prehliadači štyri závažné zraniteľnosti. Zraniteľnosť CVE-2019-5785 zapríčinená pretečením rozsahu celých čísel pri určitých operáciách v grafickej knižnici Skia môže byť potenciálne zneužitá na vykonanie škodlivého kódu alebo môže spôsobiť pád aplikácie. Zraniteľnosť CVE-2018-18356 v grafickej knižnici Skia je spôsobená opätovným použitím uvoľnenej pamäte a môže byť potenciálne zneužitá na vykonanie škodlivého kódu alebo môže spôsobiť pád aplikácie. CVE-2018-18511 je spôsobená čítaním cross-origin obrázkov z elementu canvas, čím umožňuje obídenie obmedzenia same-origin.

Zraniteľné systémy:

Mozilla Firefox 65.0.1
Mozilla Firefox ESR 60.5.1

Odporúčania:

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

Zdroje:

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

https://www.mozilla.org/en-US/security/advisories/mfsa2019-04/

https://www.mozilla.org/en-US/security/advisories/mfsa2019-05/

Google Chrome

Spoločnosť Google vydala tento mesiac aktualizáciu, ktorá opravuje zraniteľnosť CVE-2019-5784 spôsobenú nevhodnou implementáciou vo V8.

Zraniteľné systémy:

Google Chrome verzie staršie ako 72.0.3626.96

Odporúčania:

Vzhľadom na zraniteľnosť odporúčame aktualizáciu.

Zdroje:

https://chromereleases.googleblog.com/2019/02/stable-channel-update-for-desktop.html

4. Adobe Flash Player, Acrobat a Reader

Adobe Acrobat a Reader

Adobe zverejnil update pre Adobe Acrobat a Reader na operačných systémoch Windows, ktorý slúži na zabezpečenie kritických a vážnych zraniteľností. Zneužitie zraniteľnosti CVE-2019-7020, CVE-2019-7085 a ďalších umožňuje útočníkovi spustiť škodlivý kód bez vedomia používateľa. Zraniteľnosť CVE-2019-7089 umožňuje spôsobiť únik dát a CVE-2018-19725 umožňuje zvýšenie oprávnení.

Zraniteľné systémy:

Acrobat DC 2019.010.20069 a staršie
Acrobat Reader DC 2019.010.20069 a staršie
Acrobat 2017 2017.011.30113 a staršie
Acrobat Reader 2017.011.30113 a staršie
Acrobat DC 2015.006.30464 a staršie
Acrobat Reader DC 2015.006.30464 a staršie

Adobe Flash Player

Pre Adobe Flash Player bola zverejnená aktualizácia opravujúca vážnu zraniteľnosť CVE-2019-7090. Táto zraniteľnosť bola spôsobená čítaním pamäte mimo hraníc a umožňovala únik používateľských informácií.

Zraniteľné systémy:

Acrobat Flash Player Desktop Runtime 32.0.0.114 a staršie
Acrobat Flash Player for Google Chrome 32.0.0.114 a staršie
Acrobat Flash Player for Microsoft Edge and Internet Explorer 32.0.0.114 a staršie

Odporúčania:

Odporúča sa používateľom aktualizovať si softvér na najnovšiu verziu.

Zdroje:

https://helpx.adobe.com/security/products/acrobat/apsb19-13.html

https://helpx.adobe.com/security/products/acrobat/apsb19-07.html

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

https://helpx.adobe.com/security/products/flash-player/apsb19-06.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 február 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

Dirty Sock - vytvorte si v Linuxe rootovský účet

Zraniteľnosť Dirty Sock postihuje distribúcie Linuxu používajúce službu snapd, najmä Ubuntu, a dovoľuje lokálne zvýšenie práv. Je tak možné vytvoriť nový účet s právami root, pričom útočník k tomu môže využiť škodlivý balíček .snap, ktorý obeť stiahne a nainštaluje. Dôsledkom tejto zraniteľnosti je vytváranie používateľských účtov s právami root a prevzatie kontroly nad operačným systémom. Pre viac informácií si môžete prečítať naše varovanie.

Zraniteľné systémy:
Snapd verzie 2.28 až 2.37 (niekoľko distribúcií Linux, ktoré ich využívajú - najmä Ubuntu, no tiež Debian, Arch Linux, OpenSUSE, Solus a Fedora)

Odporúčania:

Aktualizácia Snapd aspoň na verziu 2.37.1

Zdroje:

https://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=229
https://www.zdnet.com/article/dirty-sock-vulnerability-lets-attackers-gain-root-access-on-linux-systems/
https://threatpost.com/dirty-sock-snapd-linux/141779/
https://gbhackers.com/dirty-sock-linux-systems/
https://betanews.com/2019/02/13/dirty-sock-snapd-linux/

WordPress: vzdialené vykonávanie kódu

Šesť rokov stará kritická zraniteľnosť umožňujúca vzdialené vykonávanie kódu bola nájdená v CMS WordPress. K vykonávaniu PHP kódu môže dôjsť zneužitím možnosti traverzovania medzi priečinkami a vloženia lokálneho súboru (local file inclusion). Útočník môže prevziať kontrolu nad serverom, na ktorom webstránka beží.

Zraniteľné systémy:

WordPress WordPress 4.9.9 a 5.0.1 ak je nainštalovaný niektorý zraniteľný modul

Odporúčania:

Opravná aktualizácia zatiaľ nie je k dispozícii, no očakáva sa jej implementácia v nasledujúcej verzii WordPress. Verzie 4.9.9 a 5.0.1 majú implementované opatrenia, ktoré zabraňujú neautorizovaným používateľom nastavovať Post Meta vstupy. Napriek tomu však zraniteľný prídavný modul (akých existuje niekoľko) môže opätovne umožniť zneužitie popísanej zraniteľnosti.

Zdroje:

https://blog.ripstech.com/2019/wordpress-image-remote-code-execution/
https://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=231

WordPress: doplnok Simple Social Buttons dovoľuje prevziať kontrolu nad stránkou

Modul pre WordPress "Simple Social Buttons" nekontroluje dostatočne používateľské práva a umožňuje tak meniť inštalačné nastavenia aj používateľom s najnižšími právami. Registrovaný používateľ môže ovládnuť administrátorský účet, alebo celú webstránku.

Zraniteľné systémy:

Wordpress doplnok Simple Social Buttons verzie od 2.0.4 po jednu nižšie ako 2.0.22

Odporúčania:

Aktualizácia aspoň na verziu 2.0.22

Zdroje:

https://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=230
https://www.webarxsecurity.com/wordpress-plugin-simple-social-buttons/
https://threatpost.com/wordpress-plugin-flaw-website-takeover/141746/
https://www.zdnet.com/article/wordpress-plugin-flaw-lets-you-take-over-entire-sites/

Zraniteľnosti obľúbených manažérov hesiel

Bezpečnostný tím spoločnosti Independent Security Evaluators skúmal zraniteľnosti štyroch obľúbených manažérov hesiel. Odhalil chyby pri odstraňovaní citlivých údajov z pamäte. Technikami memory scraping sa im podarilo získať hlavné heslo, aj heslá načítané do pamäte zo šifrovanej databázy. Pre zneužitie zraniteľností je však potrebný lokálny prístup k počítaču obete. Sami autori štúdie však odporúčajú naďalej používať softvér na manažment hesiel.

Zraniteľné systémy:

Študované verzie programov vo Windows 10:

- 1Password4 for Windows v. 4.6.2.626
- 1Password7 for Windows v. 7.2.576
- Dashlane for Windows v.6.1843.0
- KeePass Password Safe v.2.40
- LastPass for Applications v. 4.1.59

Odporúčania:

Nepredpokladá sa, že zraniteľnosti budú zneužívané, no odporúčame nainštalovať aktualizácie, keď budú dostupné.

Zdroje:

https://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=233
https://www.securityevaluators.com/casestudies/password-manager-hacking/
https://www.zdnet.com/article/critical-vulnerabilities-uncovered-in-popular-password-managers/

Kritická zraniteľnosť v CMS Drupal dovoľuje vzdialené vykonávanie kódu

Spoločnosť Drupal vydala aktualizácie na kritickú zraniteľnosť vo svojom CMS umožňujúcu vzdialene vykonávať PHP kód a následne prevziať kontrolu nad webstránkou. Zraniteľnosť sa nachádza vo verziách 8.x a niektorých prídavných moduloch. Krátko po vydaní opráv boli

zaznamenané pokusy o jej zneužitie a implantovanie skriptov na ťažbu kryptomien do zraniteľných webstránok.

Zraniteľné systémy:

Drupal 8.5.x, 8.6.x Drupal 7, ak obsahuje zraniteľné moduly (contributed projects).

Odporúčania:

- Aktualizácia Drupal aspoň na verzie 8.5.11 a 8.6.10 (staršie verzie 8.x už nie sú podporované). Aktualizovať treba aj prídavné moduly (contributed modules).
- Vypnúť moduly webových služieb, alebo nakonfigurovať webové serveri aby nepovoľovali GET/PUT/PATCH/POST požiadavky zdrojom webových služieb. Tieto zdroje môžu byť dostupné z viacerých ciest, podľa konfigurácie servera. V Drupal 7 sú dostupné z URL a cez argumenty k argumentu "q" - query; pre verziu 8 môžu cesty stále fungovať s predponou "index.php/"

Zdroje:

https://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=232
https://www.bleepingcomputer.com/news/security/drupal-fixes-highly-critical-vulnerability/
https://www.zdnet.com/article/drupal-critical-flaw-patch-this-remote-code-execution-bug-urgently-websites-warned/
https://www.zdnet.com/article/it-took-hackers-only-three-days-to-start-exploiting-latest-drupal-bug/
https://www.drupal.org/sa-core-2019-003