Mesačný prehľad kritických zraniteľností
Apríl 2019

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci apríl 8 kritických zraniteľností.

Zraniteľnosť CVE-2019-0790, CVE-2019-0791, CVE-2019-0792, CVE-2019-0793, CVE-2019-0795 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 emaili.

Ďalšou zraniteľnosťou je CVE-2019-0786 vo Windows Hyper-V. Zraniteľnosť nastáva ak hostiteľský server nevhodne zvaliduje dáta vSMB paketu. Po zneužití dokáže útočník vzdialene vykonávať kód na zraniteľnom systéme. Je potrebné, aby útočník spustil na virtuálnom stroji upravenú aplikáciu, ktorá zapríčiní, že Hyper-V systém vykoná ľubovoľný kód.

Opravená bola aj zraniteľnosť CVE-2019-0853 v komponente Graphics Device Interface (GDI+). Táto zraniteľnosť vzniká pri pristupovaní komponentu ku objektom v pamäti a umožňuje vzdialené vykonávanie kódu. Po zneužití zraniteľnosti môže útočník získať kontrolu nad zraniteľným systémom. Na napadnutie systému cez internet je potrebné, aby útočník hostil webovú stránku, ktorá je upravená na zneužitie tejto zraniteľnosti a aby presvedčil používateľa navštíviť ju (napríklad kliknutím na odkaz, ktorý na ňu smeruje). Napadnúť systém je možné aj cez zdieľanie dokumentu, ktorý je tiež upravený na zneužitie zraniteľnosti. Potom už len útočníkovi stačí presvedčiť používateľa, aby ho otvoril.

Zraniteľnosť CVE-2019-0845, umožňujúca vzdialené vykonávanie kódu, vzniká, ak IOIeCvt interface vykresľuje ASP obsah na webovej stránke. Ak útočník zneužije túto zraniteľnosť, dokáže vykonávať vzdialene akýkoľvek škodlivý kód a získať kontrolu nad napadnutým systémom. Na zneužitie tejto zraniteľnosti je potrebné hostiť webstránku, ktorej obsah je prispôsobený na využitie danej zraniteľnosti cez internetové prehliadače spoločnosti Microsoft. 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.

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.

Koniec podpory pre Windows Embedded Standard 2009

Bezplatná bezpečnostná podpora pre posledný operačný systém Windows XP, Windows Embedded POSReady 2009 v mesiaci apríl skončila. Týka sa to verzie pre pokladničné systémy.

Operačný systém Windows XP bol jedenásť rokov najpoužívanejším operačným systémom na osobných počítačoch. V roku 2012 ho predbehol Windows 7.
Neplatená podpora pre verzie Home a Professional skončila v roku 2014. Neskôr skončila podpora pre Windows Embedded Standard 2009 a tento mesiac pre Windows Embedded POSReady 2009.

Zdroje:

https://portal.msrc.microsoft.com/en-us/security-guidance
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0791
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0790
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0786
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0792
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0793
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0795
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0853
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0845
http://www.dsl.sk/article.php?article=22368

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft tento mesiac opravila 10 závažných zraniteľností.

Prvou z nich je CVE-2019-0801 a umožňuje vzdialené vykonávanie kódu. Vzniká, keď Microsoft Office nevhodne pristupuje k určitým súborom. Aby bola zraniteľnosť zneužitá, je potrebné presvedčiť používateľa, aby otvoril špeciálne upravený URL súbor, ktorý ukazuje na Excel alebo PowerPoint súbor, ktorý bol taktiež stiahnutý.

Druhou je CVE-2019-0822. Táto zraniteľnosť vzniká, ak Microsoft Graphics Components pristupuje ku objektom v pamäti. Ak útočník zneužije túto zraniteľnosť, môže vykonávať ľubovoľný kód na napadnutom systéme. Stačí, keď používateľ otvorí špeciálne upravený súbor.

Zraniteľnosť umožňujúca vzdialené vykonávanie kódu CVE-2019-8328 je spôsobená tým, že Microsoft Excel nesprávne narába s objektmi v pamäti. Na zneužitie môže útočník použiť špeciálne pripravený súbor. Potom musí ešte presvedčiť používateľa, aby tento súbor otvoril. To môže urobiť tak, že ho zašle pomocou e-mailu alebo rýchlej správy. Útočník môže taktiež využiť špeciálne vytvorenú stránku, pričom odkaz na ňu pošle používateľovi, aby ho tak presvedčil nech ju navštívi. Po úspešnom zneužití tejto zraniteľnosti, môže útočník získať

právo spúšťať škodlivý kód ako práve prihlásený používateľ. V prípade, že bol používateľ prihlásený ako administrátor získa útočník možnosť inštalovať programy; zobrazovať, meniť alebo mazať dáta; či vytvárať plnohodnotné účty.

Cross-site skriptovacia (XSS) zraniteľnosť CVE-2019-0830, CVE-2019-0831 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.

Ďalšie zraniteľnosti CVE-2019-0823, CVE-2019-0824, CVE-2019-0825, CVE-2019-0826, CVE-2019-0827 vznikajú, keď Microsoft Office Access Connectivity Engine (MOACE) nevhodne pristupuje ku objektom v pamäti. Útočníkovi umožňujú vzdialene vykonávať kód na zraniteľnom systéme. Útočník môže zraniteľnosti zneužiť, ak naláka obeť, aby otvorila infikovaný súbor.

Zraniteľné systémy:

Microsoft Office 2010 Service Pack 2 (64-bit editions)
Microsoft Office 2010 Service Pack 2 (32-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 2016 for Mac
Microsoft Office 2019 for 32-bit editions
Microsoft Office 2019 for 64-bit editions
Microsoft Office 2019 for Mac
Office 365 ProPlus for 32-bit Systems
Office 365 ProPlus for 64-bit 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-2019-0801

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0822
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0828
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0830
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0831
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0823
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0824
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0825
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0826
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0827

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft opravila v mesiaci apríl 1 kritickú zraniteľnosť.

Zraniteľnosť CVE-2019-0753 umožňuje vzdialené vykonávanie kódu, pretože skriptovací nástroj 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. Navyše 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-2019-0753

Microsoft Edge

Spoločnosť Microsoft opravila tento mesiac 7 kritických zraniteľností. Zraniteľnosť CVE-2019-0739, CVE-2019-0806, CVE-2019-0810, CVE-2019-0812, CVE-2019-0829, CVE-2019-0860, CVE-2019-0861 umožňuje vzdialené vykonávanie kódu, pretože 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-2019-0739
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0806
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0810
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0812
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0829
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0860
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0861

Mozilla Firefox

V mesiaci apríl nevydala spoločnosť Mozilla žiadne aktualizácie opravujúce zraniteľnosti.

Zdroje:

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

Google Chrome

Spoločnosť Google opravila v mesiaci apríl 37 zraniteľností. Z nich bolo 5 závažných. Zraniteľnosti CVE-2019-5809, CVE-2019-5808, CVE-2019-5805 sú typu „use-after-free“ (použitie odalokovaného miesta v pamäti), CVE-2019-5807 vzniká pri poškodení pamäte vo V8 a CVE-2019-5806 celočíselným pretečením v Angle.

Zraniteľné systémy:

Google Chrome verzie staršie ako 74.0.3729.108

Odporúčania:

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

Zdroje:

https://chromereleases.googleblog.com/2019
https://chromereleases.googleblog.com/2019/04/stable-channel-update-for-desktop_23.html

4. Adobe Flash Player, Acrobat a Reader

Adobe Flash Acrobat a Reader

Adobe zverejnil update pre Adobe Acrobat a Reader na operačných systémoch Windows, ktorý slúži na zabezpečenie kritických a závažných zraniteľností. Kritické zraniteľnosti CVE-2019-7088, CVE-2019-7112, CVE-2019-7113, CVE-2019-7125, CVE-2019-7117, CVE-2019-7128 umožňujú vykonávať ľubovoľný kód. Prvé dve zraniteľnosti sú typu „use-after-free“ (používanie odalokovaného miesta v pamäti), druhé dve vznikajú pri pretečení haldy a posledné dve pri nezhode typov. Kritická zraniteľnosť CVE-2019-7111 a ďalšie umožňuje taktiež vykonávať kód a vzniká pri zapisovaní do pamäte mimo hraníc. Posledných 10 zraniteľností je závažných. Sú spôsobené čítaním pamäte mimo hraníc a umožňujú únik používateľských informácií.

Zraniteľné systémy:

Acrobat DC 2019.010.20098 a staršie

Acrobat Reader DC 2019.010.20098 a staršie
Acrobat 2017 2017.011.30127 a staršie
Acrobat Reader 2017.011.30127 a staršie
Acrobat DC 2015.006.30482 a staršie
Acrobat Reader DC 2015.006.30482 a staršie

Adobe Flash Player

Pre Adobe Flash Player bola zverejnená aktualizácia opravujúca kritickú zraniteľnosť CVE-2019-7096. Táto zraniteľnosť bola typu „use-after-free“, (používanie odalokovaného miesta v pamäti) a umožňuje vykonávať útočníkom ľubovoľný kód. Opravená je aj závažná zraniteľnosť CVE-2019-7108, ktorá je spôsobená čítaním pamäte mimo hraníc a umožňuje únik používateľských informácií.

Zraniteľné systémy:
Adobe Flash Player Desktop Runtime 32.0.0.156 a staršie
Adobe Flash Player for Google Chrome 32.0.0.156 a staršie
Adobe Flash Player for Microsoft Edge and Internet Explorer 11 32.0.0.156 a staršie

Odporúčania:
Používateľom odporúčame aktualizovať softvér na najnovšiu verziu.

Zdroje:
https://helpx.adobe.com/security.html
https://helpx.adobe.com/security/products/flash-player/apsb19-19.html
https://helpx.adobe.com/security/products/acrobat/apsb19-17.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 vydala v mesiaci apríl plánovanú štvrťročnú veľkú sadu aktualizácií. V produkte Java SE a Java SE Embedded boli opravené 3 kritické zraniteľnosti CVE-2019-2699, CVE-2019-2697, CVE-2019-2698 a dve závažné CVE-2019-2602, CVE-2019-2684.

Zraniteľné systémy:

Java Advanced Management Console 2.12
Java SE 7u211, 8u202, 11.0.2, 12
Java SE Embedded 8u201

Odporúčania:

Odporúčame aktualizovať zraniteľné verzie Java SE a Java SE Embedded na aktuálne verzie, prostredníctvom Java Auto Update alebo na stránke spoločnosti Oracle, viď prvý odkaz v zdrojoch.

Zdroje:

https://www.oracle.com/technetwork/topics/security/alerts-086861.html
https://www.oracle.com/technetwork/security-advisory/cpuapr2019-5072813.html#AppendixJAVA

6. Iné závažné zraniteľnosti

ZERO-DAY ZRANITEĽNOSŤ V ORACLE WEBLOGIC

Okrem iného bola opravená aj zero-day zraniteľnosť CVE-2019-2725. Objavená bola výskumníkmi z KnownSec404. Ako je možné zneužitie tejto zraniteľnosti vysvetľujú čínski vývojári z oblasti informačnej bezpečnosti: „Keďže má balík WAR chybu v deserializácii vstupných informácií, útočník môže získať oprávnenia cieľového servera tým, že odošle starostlivo vytvorenú škodlivú HTTP požiadavku a vzdialene spustí príkaz bez autorizácie.“

Oracle WebLogic je založený na jazyku Java. Populárny je v prostredí cloudu aj v bežných prostrediach. Umožňuje podnikom rýchlo nasadiť nové produkty hlavne vďaka jeho škálovateľnosti. Zraniteľnosť vzniká, ak je zapnutý komponent "wls9_async_response.war" a "wls-wsat.war". Po jej zneužití dokážu útočníci vzdialene vykonávať škodlivý kód.

Dôsledky:

Vzdialené vykonávanie kódu

Závažnosť:

kritická

Odporúčanie:

Odporúčame aktualizovať na najnovšiu verziu.

Zraniteľné systémy:

WebLogic 10.X

WebLogic 12.1.3

Zdroje:

https://securityaffairs.co/wordpress/84450/breaking-news/oracle-weblogic-zeroday.html
https://www.oracle.com/technetwork/security-advisory/alert-cve-2019-2725-5466295.html?from=timeline
https://thehackernews.com/2019/04/oracle-weblogic-hacking.html

WPA3 - nechránené WI-FI heslá

Kvôli nedostatkom vo WPA3 protokole dokážu útočníci zistiť heslá wi-fi siete a odpočúvať komunikáciu medzi zariadeniami pripojenými na danej sieti. Takto môžu získať čísla kreditných kariet, heslá, čítať správy a emaily, a pristupovať k ďalším odoslaným citlivým informáciám.

Dôsledky:

- Odpočúvanie sieťovej komunikácie
- Získanie dôverných informácií používateľa
- DoS útoky na zariadenie používateľa

Opis činnosti:

CVE-2019-9494

WPA (Wi-Fi Protected Access) protokol je navrhnutý na autentifikáciu zariadení, ktoré sú pripojené cez wi-fi a používajú šifrovací protokol AES (Advanced Encryption Standard). Chráni sieť pred útočníkmi, ktorí by ich inak mohli odpočúvať komunikáciu. Pred necelým rokom bola vydaná nová verzia, WPA3, ktorá má za úlohu odstrániť závažné zraniteľnosti vo verzii WPA2. Namiesto predzdieľaného kľúča využíva technológiu SAE (Simultaneous Authentication of Equals). Vzhľadom na to, že staršiu verziu používa množstvo zariadení, novšie zariadenia podporujúce WPA3 ponúkajú aj prechodný mód umožňujúci spojenie medzi WPA2 a WPA3-SAE.

Práve tento mód obsahuje zraniteľnosti umožňujúce vykonávať niekoľko foriem útokov. Bezpečnostní výskumníci Mathy Vanhoef a Eyal Ronen vo svojom článku nazvanom Dragonblood informovali o dvoch degradačných útokoch, z ktorých jeden degraduje verziu protokolu a druhý šifrovanie v samotnom podaní rúk SAE, známom tiež ako Dragonfly. Útočník môže zneužiť prechodový mód tak, že vytvorí prístupový bod podporujúci len WPA2,

čo spôsobí použitie tohto protokolu aj v zariadení s podporou WPA3. Pri podaní rúk nového protokolu Dragonfly je terčom útokov šifrovacia metóda protokolu, pričom je možné degradovať použitú eliptickú krivku. Útočníkovi na realizovanie týchto stačí poznať SSID siete.

Zraniteľné systémy:

Systémy podporujúce protokol WPA3 a EAP-pwd

Závažnosť zraniteľnosti:

Vysoká

Možné škody:

Únik informácii

Narušenie dostupnosti systému (Dos)

Odporúčania:

Zraniteľnosti možno odstrániť aktualizáciou firmvéru na zariadeniach podporujúcich WPA3. Táto nemá vplyv na spolupracovanie zariadení.

Odkazy:

https://thehackernews.com/2019/04/wpa3-hack-wifi-password.html
https://www.bleepingcomputer.com/news/security/wpa3-wi-fi-standard-affected-by-new-dragonblood-vulnerabilities/
https://arstechnica.com/information-technology/2019/04/serious-flaws-leave-wpa3-vulnerable-to-hacks-that-steal-wi-fi-passwords/
https://papers.mathyvanhoef.com/dragonblood.pdf

Zero-day na TP-Link Smart Home Router

Zero-day zraniteľnosť v routeroch TP-Link SR20 umožňuje útočníkom vykonávať ľubovoľný kód. Súvisí s procesom TDDP, ktorý zvyčajne beží s právami root. Zneužiť je ju možné cez lokálnu sieť. Zatiaľ neexistuje opravná aktualizácia.

Dôsledky:

- Vykonávanie ľubovoľného kódu s právami root
- Prevzatie kontroly nad zariadením

Opis činnosti:

Nová zero-day zraniteľnosť bola objavená na routeri SR20 Smart Home Router od spoločnosti TP-Link. Dôsledkom zraniteľnosti je vykonávanie ľubovoľného kódu na

zariadeniach pripojených do tej istej LAN siete. Z externej siete nie je pri prednastavených firewall pravidlách možné zraniteľnosť zneužiť.

Matthew Garrett zo spoločnosti Google najprv zraniteľnosť nahlásil spoločnosti TP-Link, avšak keďže nepodnikla žiadne kroky na opravu, po 90 dňoch zverejnil jej existenciu na sociálnej sieti Twitter. Takisto zverejnil funkčný dôkaz zraniteľnosti. Zraniteľnosť sa nachádza v procese s názvom TDDP (TP-Link Device Debug Protocol), ktorý je často spúšťaný s právami root. Tento proces bol v minulosti prameňom aj ďalších zraniteľností.

TDDP proces umožňuje vykonávanie príkazov, ktoré nepotrebujú autentifikáciu používateľa, aj príkazov, ktoré vyžadujú administrátorskú autentifikáciu. Práve medzi prvý typ patria aj príkazy súvisiace s validáciou nastavení. Útočník ich dokáže zneužiť a poslať príkaz s menom súboru a argumentom. TP-Link router ho pošle cez TFTP protokol (Trivial File Transfer Protocol). Na zariadení útočníka si vyžiada názov súboru, ktorý útočník sám zadal, a odošle proces ďalej do LUA interpretera, ktorý beží s právami root. Neskôr metóda os.execute() umožní aj neautentifikovanému útočníkovi vykonávať ľubovoľné príkazy s právami root. To môže viesť až k prevzatiu kontroly nad zraniteľným TP-Link SR20 zariadením.

Vzhľadom na to, že proces TDDP využívajú viaceré modely TP-Link routerov, zraniteľnosť môže existovať aj u nich.

Zraniteľné systémy:

SR20 Smart Home Router od spoločnosti TP-Link, prípadne ďalšie modely využívajúce proces TDDP

Závažnosť zraniteľnosti:

Vysoká

Možné škody:

Vzdialené vykonávanie kódu

Odporúčania:

Nie je vydaná žiadna nová aktualizácia, no posledná verzia z júna 2018 pre SR20 Smart Home Router opravila viaceré chyby a pridala podporu pre veľký počet TP-Link Smart Wifi zariadení. Odporúča sa aktualizovať aspoň na túto verziu.

Odkazy:

https://www.bleepingcomputer.com/news/security/zero-day-tp-link-sr20-router-vulnerability-disclosed-by-google-dev/
https://www.securityweek.com/0-day-tp-link-sr20-routers-allows-command-execution

Kritická zraniteľnosť na serveri Apache dovoľuje vykonávať kód

Kritická zraniteľnosť v aplikácii Apache server umožňuje vďaka dedeniu práv procesov zvýšiť útočníkom práva až na root a tak vykonávať kód. Nebezpečná je najmä pre služby poskytujúce webový hosting, nakoľko útočník môže kompromitovať hostované webstránky. Zraniteľnosť je zneužiteľná na Unixových systémoch.

Dôsledky:

- Vykonávanie kódu s právami root
- Kompromitovanie stránok na serveri
- Prihlásenie sa pod iným menom
- Vyhnutie sa kontrole prístupu

Opis činnosti:

CVE-2019-0211

Na serveri Apache bola objavená nová zraniteľnosť CVE-2019-0211. Postaral sa o to výskumník spoločnosti Ambionics Security, Charles Fol. Apache je jedným z najvyužívanejších open-source webových serverov. Zraniteľnosť umožňuje bežným používateľom vykonávať ľubovoľný kód cez manipuláciu s výsledkovou tabuľkou (scoreboard). Spustia „detský“ proces, na ktorý majú oprávnenia. Ten sa však vykoná s právami rodičovského procesu (čo je zvyčajne root). Získajú tak možnosť vykonávať kód s právami root. Systémy, ktoré nepoužívajú UNIX, nie sú zraniteľné. Charles Fol ešte nezverejnil funkčnú ukážku zneužitia zraniteľnosti, no spísal postup na jej zneužitie:

- Získanie oprávnení na čítanie a zapisovanie procesu
- Napísanie falošnej štruktúry prefork_child_bucket do SHM
- Dosiahnuť, aby all_buckets[bucket] ukazoval na danú štruktúru
- Počkať do 6:25. Vtedy budete môcť spustiť ľubovoľné funkčné volanie

Táto zraniteľnosť zasahuje hlavne služby poskytujúce zdieľaný webový hosting, pretože útočníci s možnosťou vykonávať PHP alebo CGI kód majú vďaka nej možnosť získať prístup na server s právami root a nakoniec kompromitovať všetky webové stránky na danom serveri.

V najnovšej verzii sú opravené ďalšie dve závažné zraniteľnosti. CVE-2019-0217 umožňuje používateľovi s platnými prihlasovacími údajmi prihlásiť sa pod iným menom a obísť bezpečnostnú kontrolu prístupu. CVE-2019-0215 sa nachádza v mod_sll. Vzniká pri verifikácii klientskeho certifikátu pomocou TLSv1.3 a umožňuje obísť nakonfigurované kontroly prístupu.

Opravených bolo aj viacero zraniteľností s nízkou závažnosťou.

Zraniteľné systémy:

Apache HTTP Server systémy verzie 2.4.17 až 2.4.38

Závažnosť zraniteľnosti:

Vysoká

Možné škody:

Únik informácii

Vzdialené vykonávanie kódu

Odporúčania:

Odporúčame aktualizovať Apache HTTP server na verziu 2.4.39

Odkazy:

https://thehackernews.com/2019/04/apache-web-server-security.html
https://www.bleepingcomputer.com/news/security/apache-bug-lets-normal-users-gain-root-access-via-scripts/
https://securityaffairs.co/wordpress/83225/hacking/cve-2019-0211-apache-flaw-allows-getting-root-access-via-script.html/

Kritické zraniteľnosti CMS Magento

V populárnom CMS Magento bolo opravených 37 zraniteľností, z ktorých štyri boli označené ako kritické a štyri ako závažné. Umožňujú vykonávať XSS a CSRF útoky, vzdialene vykonávať kód, či manipulovať s databázou webstránky pomocou SQL injekcie. Útočník môže získať citlivé údaje vrátane administrátorských prístupov a prevziať kontrolu nad stránkou.

Dôsledky:

- Prístup ku dôverným informáciám
- Vzdialené vykonávanie kódu
- Prevzatie kontroly nad webstránkou

Opis činnosti:

Magento je jednou z najpopulárnejších (nielen) e-commerce content management system (CMS) platforiem. Vývojárska spoločnosť vydala nové aktualizácie na opravu 37 objavených zraniteľností, ktoré umožňujú únik informácií, XSS a CSRF útoky, vzdialené vykonávanie kódu, či zvýšenie práv. Väčšina je zneužiteľná len autentifikovanými používateľmi s istým stupňom práv.

Jedna z najzávažnejších zraniteľností, ktorú dokážu zneužiť aj neautentifikovaní vzdialení útočníci, umožňuje manipulácie s dátami v databáze pomocou SQL injekcie. Zraniteľná je metóda prepareSqlCondition v triede Magento\Framework\DB\Adapter\Pdo\Mysql. Útočníci po jej zneužití môžu vzdialene vykonávať kód, či získať prístup ku dôverným informáciám zraniteľných e-commerce webových stránok, akými sú hashe hesiel, história objednávok a platobné údaje používateľa. Môžu tiež získať údaje potrebné pre prihlásenie do administrátorského rozhrania.

Najkritickejšie zraniteľnosti vyžadujúce pre zneužitie autentifikáciu umožňujú vzdialené vykonávanie ľubovoľného kódu s využitím škodlivého newsletteru, alebo e-mailovej šablóny; či stored cross-site scripting (XSS), ktorá dovoľuje útočníkovi vložiť škodlivý kód na stránku.

Zraniteľné systémy:

- Magento Open Source verzie pred 1.9.4.1
- Magento Commerce verzie pred 1.14.4.1
- Magento Commerce 2.1 verzie pred 2.1.17
- Magento Commerce 2.2 verzie pred 2.2.8
- Magento Commerce 2.3 verzie pred 2.3.1

Závažnosť zraniteľnosti:

Vysoká

Možné škody:

Únik informácii

Vzdialené vykonávanie kódu

Odporúčania:

Magento odporúča bezodkladnú aktualizáciu CMS na najnovšiu verziu (2.3.1, 2.2.8 a 2.1.17).

Odkazy:

https://thehackernews.com/2019/03/magento-website-security.html
https://www.securityweek.com/magento-patches-critical-vulnerabilities
https://threatpost.com/magento-xss-csrf-rce-vulnerabilities/143274/

Aplikácia Signal - zraniteľnosť Homograph Domain

V aplikácii pre bezpečnú komunikáciu Signal existuje zraniteľnosť pri nedostatočnom overovaní používateľských vstupov, ktorá dovoľuje zneužiť homografy pri registrovaní podvodných domén a presvedčiť tak obeť, že pristupuje na legitímnu webstránku.

Dôsledky:

Oklamanie používateľa, že webstránka, na ktorú pristupuje, je legitímna, pričom sa jedná o doménu pod kontrolou útočníka.

Opis činnosti:

CVE-2019-9970

Zraniteľnosť v aplikácii Signal, ktorá je zameraná na bezpečnú komunikáciu, existuje, pretože aplikácia nesprávne spracováva homografy v doménach medzinárodných doménových mien (International Domain Name (IDN)). Útočník ju môže zneužiť pri sociálnom inžinierstve na tzv. spoofingový útok na doménu. Obeti podvrhne do komunikácie doménu, ktorá sa tvári ako legitímna. Často používaným trikom útočníkov je zaregistrovanie domény, ktorá obsahuje znaky medzinárodných sád Unicode vizuálne podobné ASCII znakom. Keďže tieto znaky sú vizuálne ťažko rozlíšiteľné, útočníci majú veľkú šancu, že obeť si neuvedomí, že pristupuje na škodlivú doménu. Bola zverejnená aj funkčná ukážka, ktorou vývojári dokázali zraniteľnosť aplikácie.

Zraniteľné systémy:

Signal Desktop verzie 1.23.1 a staršej

Signal Private Messenger verzie 4.35.3 a staršej

Závažnosť zraniteľnosti:

Vysoká

Možné škody:

Phishing
Únik informácií

Odporúčania:

Aktualizácia na najnovšiu verziu.

Odkazy:

http://www.digitalmunition.me/2019/03/signal-cve-2019-9970-homograph-domain-spoofing-vulnerability/
https://medium.com/@digitalmunition/signal-cve-2019-9970-homograph-domain-spoofing-vulnerability-54c37eae1ebc
https://www.securityfocus.com/bid/107550
https://portswigger.net/daily-swig/lookalike-domain-phishing-attacks-threaten-signal-and-telegram-users