Mesačný prehľad kritických zraniteľností
September 2018

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft tento mesiac opravila päť kritických zraniteľností týkajúcich sa operačného systému Windows. Každá z týchto zraniteľností umožňuje útočníkovi vzdialene vykonávať kód.

CVE-2018-8475 nastáva pretože Windows nesprávne narába so špeciálne upravenými obrázkami. Na jej zneužitie musí útočník presvedčiť používateľa aby stiahol obrázok. Zraniteľnosti CVE-2018-8439 a CVE-2018-0965 nastávajú keď sú nesprávne spracované vstupy od používateľa pomocou Windows Hyper-V na serveri. Zneužiť túto zraniteľnosť je možné tak, že útočník spustí špeciálne pripravenú aplikáciu na hosťovskom operačnom systéme a tým spôsobí vzdialené vykonávanie kódu. Ďalšou opravenou zraniteľnosťou je zraniteľnosť CVE-2018-8420, ktorá nastáva keď Microsoft XML Core Services MSXML parser spracuje používateľský vstup.

Poslednou opravenou zraniteľnosťou v balíku aktualizácií bola zraniteľnosť CVE-2018-8332, ktorá nastáva nesprávnym spracovaním špeciálne vytvorených písiem knižnicou písiem systému Windows. Útočník, ktorý úspešne zneužije niektorú z týchto zraniteľností, by mohol prevziať kontrolu nad postihnutým systémom. Útočník potom môže nainštalovať programy; zobraziť, zmeniť alebo vymazať údaje; alebo vytvoriť nové účty s plnými používateľskými právami. Používatelia, ktorých účty sú nakonfigurované tak, aby mali menej používateľských práv v systéme, by mohli byť menej ovplyvnení ako používatelia, ktorí pracujú s administrátorskými používateľskými právami. Na ich zneužitie musí útočník presvedčiť používateľa, aby navštívil špeciálne pripravenú stránku, alebo otvoril špeciálne upravený dokument. To môže urobiť tým, že zašle odkaz na stránku alebo súbor používateľovi pomocou e-mailu alebo rýchlej správy.

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 x64-based Systems
Windows 10 Version 1803 for 32-bit Systems
Windows 10 Version 1803 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, version 1709 (Server Core installation)
Windows Server, version 1803 (Server Core installation)

Odporúčania:

Vzhľadom na množstvo kritických zraniteľností odporúčame bezodkladne 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-2018-0965
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8332
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8420
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8439
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8475

2. Kancelárske balíky Microsoft Office a Office Web Apps

V balíkoch Microsoft Office bola tento mesiac opravená jedna kritická a šesť závažných zraniteľností.

Zraniteľnosť označená ako kritická má označenie CVE-2018-8332 a bola spomenutá už aj v časti operačné systémy Windows.

Tri zraniteľnosti CVE-2018-8426, CVE-2018-8428 a CVE-2018-8431 sa týkajú Microsoft SharePoint servera pričom umožňujú cross-site-scripting útoky a vykonávanie skriptov ako práve prihlásený používateľ. Tieto útoky môžu ďalej spôsobiť, že útočník môže vidieť obsah na SharePoint stránke, ku ktorému nemá právo a vykonávať akcie ako zmazanie obsahu alebo vloženie obsahu.

Zraniteľnosť vzdialeného vykonávania kódu CVE-2018-8331 je spôsobená tým, že Microsoft Excel alebo Microsoft PowerPoint 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 jednej z týchto

zraniteľností, 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.
CVE-2018-8430 je zraniteľnosť vzdialeného vykonávania kódu a nastáva, keď používateľ v aplikácii Microsoft Word otvorí špeciálne upravené PDF.
Poslednou opravenou zraniteľnosťou je zraniteľnosť CVE-2018-8429, ktorá umožňuje únik informácií. Nastáva keď Microsoft Excel nesprávne zverejňuje obsah pamäte a útočník, ktorý zneužil túto zraniteľnosť má možnosť vidieť informácie, ktoré boli už vymazané z hárku.

Zraniteľné systémy:

Microsoft Excel 2016 Click-to-run 32-bitová verzia
Microsoft Excel 2016 Click-to-run 64-bitová verzia
Microsoft Excel 2010 Service Pack 2 (32-bitová verzia)
Microsoft Excel 2010 Service Pack 2 (64-bitová verzia)
Microsoft Excel 2013 RT Service Pack 1
Microsoft Excel 2013 Service Pack 1 (32-bitová verzia)
Microsoft Excel 2013 Service Pack 1 (64-bitová verzia)
Microsoft Excel 2016 (32-bitová verzia)
Microsoft Excel 2016 (64-bitová verzia)
Microsoft Excel Viewer 2007 Service Pack 3
Microsoft Office 2016 pre Mac
Microsoft Office Compatibility Pack Service Pack 3
Microsoft PowerPoint 2010 Service Pack 2 (32-bitová verzia)
Microsoft PowerPoint 2010 Service Pack 2 (64-bitová verzia)
Microsoft Office 2016 Click-to-Run (C2R) 32-bitová verzia
Microsoft Office 2016 Click-to-Run (C2R) 64-bitová verzia
Microsoft Office 2010 Service Pack 2 (32-bitová verzia)
Microsoft Office 2010 Service Pack 2 (64-bitová verzia)
Microsoft Office 2013 RT Service Pack 1
Microsoft Office 2013 Service Pack 1 (32-bitová verzia)
Microsoft Office 2013 Service Pack 1 (64-bitová verzia)
Microsoft Office 2016 (32-bitová verzia)
Microsoft Office 2016 (64-bitová verzia)
Microsoft SharePoint Enterprise Server 2013 Service Pack 1
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Server 2013 Service Pack 1
Microsoft Office Web Apps 2010 Service Pack 2
Microsoft Office Web Apps 2013 Service Pack 1
Microsoft Office Word Viewer
Word Automation Services

Odporúčania:

Vzhľadom množstvo závažných zraniteľností odporúčame bezodkladne 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-2018-8332
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8331
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8426
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8428
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8431
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8430
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8429

3. Internetové prehliadače

Microsoft Internet Explorer

Tri kritické zraniteľnosti boli opravené tento mesiac v prehliadači Internet Explorer. Zraniteľnosti môžete nájsť pod označeniami: CVE-2018-8457, CVE-2018-8461, a CVE-2018-8447. Zraniteľnosti sú spôsobené nesprávnym narábaním prehliadača Internet Explorer s objektmi v pamäti. Môžu spôsobiť také poškodenie pamäte, že útočník získa možnosť spúšťať kód ako práve prihlásený používateľ. Ak je teda práve prihláseným používateľom administrátor, získa útočník právo inštalovať programy, prezerať, mazať alebo meniť dáta, či vytvárať ďalšie plnohodnotné účty. Na ich zneužitie však útočník potrebuje interakciu používateľa, keďže ho musí presvedčiť aby navštívil špeciálne vytvorenú stránku, ktorej odkaz môže poslať napríklad pomocou emailu alebo rýchlej správy. Taktiež má možnosť vložiť do aplikácie alebo dokumentu Microsoft Office prvok ActiveX označený ako bezpečný na inicializáciu.

Zraniteľné systémy:

Microsoft Internet Explorer verzie 9, 10 a 11

Odporúčania:

Vzhľadom na závažnosť kritických zraniteľností odporúčame bezodkladne 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-2018-8461
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8447
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8457

Microsoft Edge

Osem kritických zraniteľností bolo opravených tento mesiac v prehliadači Microsoft Edge, pričom všetky umožňujú vykonať škodlivý kód na diaľku. Opravenými zraniteľnosťami sú: CVE-2018-8456, CVE-2018-8459, CVE-2018-8367, CVE-2018-8465, CVE-2018-8466, CVE-2018-8467 a CVE-2018-8464.
Všetky zraniteľnosti sú spôsobené tým, že skriptovací engine nesprávne narába s objektmi v pamäti. Zneužitie je možné len za pomoci používateľa, ktorého musí útočník presvedčiť k navštíveniu ním špeciálne vytvorenej stránky. Úspešné zneužitie týchto zraniteľností umožňuje útočníkovi prebrať kontrolu nad systémom a vykonať ľubovoľný škodlivý kód s oprávneniami práve prihláseného používateľa. V prípade, že používateľ mal administrátorské práva útočník získa možnosť inštalovať programy, prezerať, meniť a mazať dáta, prípadne vytvárať plnohodnotné používateľské účty.

Zraniteľné systémy:

Microsoft Edge v systémoch Windows 10 verzií 1607, 1703, 1709 a 1803 a 32-bitových aj 64-bitových verziách
Microsoft Edge v systémoch Windows 10 32-bitových aj 64-bitových verziách
Microsoft Edge v systéme Windows Server 2016

Odporúčania:

Vzhľadom na množstvo kritických zraniteľností odporúčame bezodkladne 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-2018-8456
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8459
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8367
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8457
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8465
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8466
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8467
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8464

Mozilla Firefox

Spoločnosť Mozilla tento mesiac opravila jednu kritickú a tri závažné zraniteľnosti. Kritickou zraniteľnosťou je CVE-2018-12376 a môže spôsobiť vzdialené vykonávanie kódu.

Zdroje:

https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2018-21/
https://www.mozilla.org/en-US/security/advisories/mfsa2018-20/

Google Chrome

Spoločnosť Google vydala tento mesiac aktualizácie, ktoré opravujú osem závažných zraniteľností.

Zdroje:
https://chromereleases.googleblog.com/2018
https://chromereleases.googleblog.com/2018/09/stable-channel-update-for-desktop.html
https://chromereleases.googleblog.com/2018/09/stable-channel-update-for-desktop_11.html

4. Adobe Flash Player

Závažná zraniteľnosť CVE-2018-15967 v produkte Adobe Flash Player bola opravená v aktualizáciách vydaných spoločnosťou Adobe tento mesiac. Opravená zraniteľnosť môže spôsobiť únik informácií a zvýšenie práv.

Zraniteľné systémy:
Adobe Flash Player Desktop Runtime 30.0.0.154 a staršie pre Windows, macOS aj Linux
Adobe Flash Player pre Google Chrome 30.0.0.154 a staršie
Adobe Flash Player pre Microsoft Edge a Internet Explorer 11 30.0.0.154 a staršie

Odporúčania:
Používateľom odporúčame čo najskôr aktualizovať Adobe Flash Player na verziu 31.0.0.108. Aktualizácie sú dostupné prostredníctvom stránky Adobe Flash Player Download Center, prípadne prostredníctvom kontroly dostupných aktualizácii v produkte Adobe Flash Player.

Zdroje:
https://helpx.adobe.com/security.html
https://helpx.adobe.com/security/products/flash-player/apsb18-31.html

5. Frameworky

Microsoft .NET Framework

V aktualizácii vydanej pre Microsoft .NET Framework bola opravená jedna kritická zraniteľnosť. Ide o zraniteľnosť s označením CVE-2018-8421, ktorá spôsobuje vzdialené vykonávanie kódu. Nastáva keď Microsoft .NET Framework spracúva vstup.

Zdroje:
https://portal.msrc.microsoft.com/en-us/security-guidance
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8421

Oracle Java

Spoločnosť Oracle nevydala v mesiaci jún žiadne aktualizácie platformy Java. Najbližšia veľká sada aktualizácií je naplánovaná na 16. október 2018.

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

6. Iné závažné zraniteľnosti

Zraniteľnosť Peekaboo

Zraniteľnosť objavená v monitorovacích systémoch NUUO umožňuje útočníkovi vzdialene vykonávať kód s administrátorskými privilégiami, sledovať a upravovať, či odpojiť živý signál z kamier a manipulovať s nahrávkami. Pre bližšie informácie o tejto zraniteľnosti si prečítajte naše varovanie.

Zraniteľné systémy:

Video manažovací softvér v IP rekordéroch NVRMini2 od spoločnosti NUUO, ktoré používa vyše 2500 typov bezpečnostných kamier od 100 výrobcov.

Odporúčania:

Aktualizácia softvéru pre NUUO NVRMini2 aspoň na verziu 3.9.1 a povoliť sieťový prístup k citlivým zariadeniam len povolaným osobám.

WordPress stránky

Bol zaznamenaný nárast počtu útokov na WordPress stránky napríklad upravením stránky tak, že používateľ bol presmerovaný na podvodné služby technickej podpory. Bližšie informácie sa dozviete v našom varovaní.

Zraniteľné systémy:

Wordpress stránky

Doplnok Snap Creek Duplicator starší ako 1.2.42

Odporúčania:

- Vymazať súbory installer.php a installer-backup.php z koreňového adresára webstránky, najmä ak boli vytvorené verziami doplnku Duplicator staršími ako 1.2.42
- Aktualizovať Duplicator aspoň na verziu 1.2.42
- Staré, nepoužívané súbory a zálohy treba z bezpečnostného hľadiska odkladať mimo aktívnej zložky webstránky, pretože môžu slúžiť ako vektor útoku.
- Ak bola stránka napadnutá (bolo zistené jej zlyhanie), je potrebné identifikovať zdroj a odstrániť ho. Oprava pripojenia databázy, ani obnovenie stránky zo zálohy nepostačuje na odstránenie hrozby.

Microsoft Jet Database Engine

Zraniteľnosť v nástroji Microsoft Jet Database Engine umožňuje vykonávať vzdialene kód v kontexte aktuálneho procesu. Pre viac informácií si prečítajte naše varovanie.

Zraniteľné systémy:

Microsoft Windows, všetky súčasné verzie vrátane verzií pre servery

Studeným štartom k informáciám zo šifrovaných diskov

Bol odhalený spôsob ako znefunkčniť softvérovú ochranu pred útokom typu cold boot (studený štart) čo umožňuje získať dáta z pamäte RAM a získať tak aj heslá a kryptografické kľúče k šifrovaným diskom. Viac informácií môžete nájsť v našom varovaní.

Zraniteľné systémy:

Pravdepodobne všetky osobné počítače okrem produktov Apple, ktoré využívajú čip T2.

Odporúčania:

Momentálne neexistuje riešenie na úplné zamedzenie možnosti útoku, no nasledujúce odporúčania výrazne znížia pravdepodobnosť úspechu.

- Zariadenia od Apple s čipom T2 by mali byť bezpečné
- Chrániť firmvér heslom
- Zakázať režim spánku (Sleep), vďaka čomu nezostanú v pamäti načítané heslá a kľúče k šifrovaným partíciám
- Pred štartovaním / zobudením systému nastaviť vyžiadanie hesla pre BitLocker

Cisco zraniteľnosti

Pre bližšie informácie o opravených zraniteľnostiach v produktoch Cisco si prečítajte naše varovanie.

Zraniteľné systémy:

RV110W Wireless-N VPN Firewall
RV130W Wireless-N Multifunction VPN Router
RV215W Wireless-N VPN Router
Cisco Umbrella service
Cisco SocialMiner
Cisco Prime Service Catalog
Cisco Identity Services Engine (ISE)
Cisco Emergency Responder
Cisco Finesse
Cisco Hosted Collaboration Solution for Contact Center
Cisco MediaSense
Cisco Unified Communications Manager IM & Presence Service (formerly CUPS)
Cisco Unified Communications Manager
Cisco Unified Contact Center Enterprise - Live Data server
Cisco Unified Contact Center Enterprise
Cisco Unified Contact Center Express
Cisco Unified Intelligence Center
Cisco Unified Intelligent Contact Management Enterprise
Cisco Unified SIP Proxy Software
Cisco Unified Survivable Remote Site Telephony Manager
Cisco Unity Connection
Cisco Virtualized Voice Browser
Cisco Video Distribution Suite for Internet Streaming (VDS-IS)
Cisco Network Performance Analysis

Odporúčania:

- **CVE-2018-0423**
  Zraniteľnosť je opravená v Cisco RV130W Wireless-N Multifunction VPN Router verzie 1.0.3.44, ktorú je možné stiahnuť z Software Center na stránke cisco.com.
- **CVE-2018-0435**
  Odporúčame aktualizovať na najnovšiu verziu.
- **CVE-2018-11776**
  Na tejto stránke môžete v sekcii zraniteľných systémov nájsť príslušné verzie, v ktorých je už zraniteľnosť opravená. Odporúčame aktualizovať na danú verziu.

Zraniteľnosť Tor 7.x

Zraniteľnosť prehliadača Tor Browser sa nachádza v predinštalovanom prídavnom module NoScript a umožňuje útočníkovi spúšťať ľubovoľný JavaScript kód. Bližšie informácie sa dočítate v našom varovaní.

Zraniteľné systémy:

Tor Browser 7.x NoScript 5.0.4 – 5.1.8.6 s nastavením „Safest“

Odporúčania:

Odporúčame aktualizovať Tor Browser aspoň na verziu 8.0 a aktualizovať NoScript aspoň na verziu 5.1.8.7.

MikroTik routery

Spoločnosťou 360 NetLAb bolo odhalené masové odpočúvanie komunikácie cez MikroTik routery. Odpočúvanie bolo možné vďaka zraniteľnosti v nástroji Winbox v MikroTik RouterOS. Po zneužití má útočník možnosť získať kontrolu nad routerom, odpočúvať sieťovú komunikáciu a vykonávať inú škodlivú činnosť. V našom varovaní môžete nájsť viac informácií o tejto zraniteľnosti.

Zraniteľné systémy:

MikroTik routre využívajúce MikroTik RouterOS verzie 6.29 – 6.42.

Odporúčania:

Aktialuzácia MikroTik RouterOS na verziu novšiu ako 6.43 a zakázanie aplikácie Winbox.