Mesačný prehľad kritických zraniteľností
Október 2018

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft tento mesiac opravila tri kritické zraniteľnosti týkajúce sa operačného systému Windows. Každá z týchto zraniteľností umožňuje útočníkovi vzdialene vykonávať kód.
Zraniteľnosti CVE-2018-8489 a CVE-2018-8490 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-2018-8494, ktorá nastáva keď Microsoft XML Core Services MSXML parser spracuje používateľský vstup.
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 ovplyvnené ako používatelia, ktorí pracujú s administrátorskými používateľskými právami. Na ich zneužitie musí útočník presvedčiť používateľa, aby navštívil špeciálne pripravenú stránku, alebo otvoril špeciálne upravenú dokument. To môže urobiť tým, že zašle odkaz na stránku alebo súbor používateľovi pomocou e-mailu alebo rýchlej správy.
Tento mesiac bola taktiež objavená chyba v aktualizácii pre Microsoft Windows 10 na verziu 1809, ktorá spôsobuje mazanie používateľských súborov v zložke Documents. Viac o tejto chybe si môžete prečítať v našom varovaní.
Spoločnosť Microsoft okrem iného opravila taktiež zero-day zraniteľnosť, ktorá umožňuje útočníkom zvýšenie privilégií, vykonávanie kódu v režime jadra, manipuláciu s dátami a vytváranie nových účtov s právami používateľa. Pre bližšie informácie o tejto zraniteľnosti si prečítajte naše varovanie.
K spomínanej opravenej zero-day zraniteľnosti pridala spoločnosť Microsoft tento mesiac ešte jednu, ktorá umožňuje zvýšiť privilégiá používateľa na úroveň administrátora a potenciálne nahradiť kritické systémové súbory upravenou škodlivou verziou. Viac informácií môžete nájsť v našom varovaní.

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 2019
Windows Server 2019 (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-2018-8494
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8490
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8489

2. Kancelárske balíky Microsoft Office a Office Web Apps

V balíkoch Microsoft Office bolo tento mesiac opravených osem závažných zraniteľností.
Tri zraniteľnosti CVE-2018-8518, CVE-2018-8488 a CVE-2018-8480 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-2018-8501, CVE-2018-8502 a CVE-2018-8504 je spôsobená tým, že Microsoft Excel, Microsoft Word alebo Microsoft PowerPoint nesprávne narábajú s objektmi v pamäti. Na zneužitie môže útočník použiť špeciálne

pripravený súbor. Potom musí ešte presvedčiť používateľa, aby ten 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.

Zraniteľnosti CVE-2018-8432 a CVE-2018-8427 vzdialeného vykonávania kódu a úniku informácií nastávajú keď Microsoft Graphics Components nesprávne narába s objektmi v pamäti.

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 PowerPoint 2010 Service Pack 2 (32-bitová verzia)
Microsoft PowerPoint 2010 Service Pack 2 (64-bitová verzia)
Microsoft PowerPoint 2013 RT Service Pack 1
Microsoft PowerPoint 2013 Service Pack 1 (32-bitová verzia)
Microsoft PowerPoint 2013 Service Pack 1 (64-bitová verzia)
Microsoft PowerPoint 2016 (32-bitová verzia)
Microsoft PowerPoint 2016 (64-bitová verzia)
Microsoft Word 2010 Service Pack 2 (32-bitová verzia)
Microsoft Word 2010 Service Pack 2 (64-bitová verzia)
Microsoft Word 2013 RT Service Pack 1
Microsoft Word 2013 Service Pack 1 (32-bitová verzia)
Microsoft Word 2013 Service Pack 1 (64-bitová verzia)
Microsoft Word 2016 (32-bitová verzia)
Microsoft Word 2016 (64-bitová verzia)
Microsoft Office 2016 pre Mac
Microsoft Office Compatibility Pack Service Pack 3
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 Office 2019 (32-bitová verzia)
Microsoft Office 2019 (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
PowerPoint Viewer 2010 (32-bitová verzia)
Word Automation Services
Office 365 ProPlus pre 32-bitové systémy
Office 365 ProPlus pre 64-bitové systémy

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-2018-8518
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8488
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8480
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8502
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8504
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8501
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8432
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8427

3. Internetové prehliadače

Microsoft Internet Explorer

Iba dve kritické zraniteľnosti boli opravené tento mesiac v prehliadači Internet Explorer. Zraniteľnosti spôsobujúce poškodenie pamäte môžete nájsť pod označeniami: CVE-2018-

8460 a CVE-2018-8491. 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.

Zraniteľné systémy:
Microsoft Internet Explorer verzie 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-2018-8460
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8491

Microsoft Edge

Šesť kritických zraniteľností bolo opravených tento mesiac v prehliadači Microsoft Edge, pričom pri zneužití týchto zraniteľností je poškodená pamäť. Opravenými zraniteľnosťami sú: CVE-2018-8473, CVE-2018-8505, CVE-2018-8509, CVE-2018-8510, CVE-2018-8511 a CVE-2018-8513. Postup zneužitia a možné dôsledky sú rovnaké ako pri zraniteľnostiach spomínaných pre Internet Explorer.

Zraniteľné systémy:
Microsoft Edge v systémoch Windows 10 verzií 1607, 1703, 1709, 1803 a 1809 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
Microsoft Edge v systéme Windows Server 2019

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-2018-8473
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8505
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8509
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8510

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8511
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8513

Mozilla Firefox

Spoločnosť Mozilla tento mesiac opravila dve kritické zraniteľnosti. Zraniteľnosť CVE-2018-12386 sa týkaj prideľovania registrov v jazyku JavaScript , čo umožní ľubovoľný zápis či čítanie. Druhá, označená ako CVE-2018-1287, sa týka kompilátora JavaScript JIT, ktorý odhalí adresu pamäte volacej funkcie pri Array.prototype.push s viacerými argumentmi.

Zdroje:

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

https://www.mozilla.org/en-US/security/advisories/mfsa2018-24/

Google Chrome

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

Zdroje:

https://chromereleases.googleblog.com/2018
https://chromereleases.googleblog.com/2018/10/stable-channel-update-for-desktop.html

4. Adobe Flash Player

Veľké množstvo kritických a závažných zraniteľností bolo tento mesiac opravených spoločnosťou Adobe v produkte Adobe Acrobat Reader. Zraniteľnosti umožňujú vzdialené vykonávanie kódu, únik informácií a zvýšenie práv. O týchto a ďalších zraniteľnostiach týkajúcich sa taktiež PDF prehliadača Foxit sa môžete dočítať viac v našom varovaní.

Zraniteľné systémy:

Acrobat DC 2018.011.20063 a staršie
Acrobat Reader DC 2018.011.20063 a staršie
Acrobat 2017 2017.011.30102 a staršie
Acrobat Reader 2017 2017.011.30102 a staršie
Acrobat DC 2015 2015.006.30452
Acrobat Reader DC 2015 2015 2015.006.30452

Odporúčania:

Používateľom odporúčame čo najskôr aktualizovať zraniteľné systémy nasledovne:

- Acrobat DC 2019.008.20071
- Acrobat Reader DC 2019.008.20071
- Acrobat 2017 2017.011.30105
- Acrobat Reader 2017 2017.011.30105
- Acrobat DC 2015 2015.006.30456
- Acrobat Reader DC 2015 2015.006.30456

Aktualizácie sú dostupné prostredníctvom stránky Adobe Acrobat Reader Download Center, prípadne prostredníctvom kontroly dostupných aktualizácii v produkte Adobe Acrobat Reader.

Zdroje:
https://helpx.adobe.com/security.html
https://helpx.adobe.com/security/products/acrobat/apsb18-30.html

5. Frameworky

Microsoft .NET Framework

V aktualizácii vydanej pre Microsoft .NET Core boli opravená jedna závažná zraniteľnosť. Ide o zraniteľnosť s označením CVE-2018-8292, ktorá spôsobuje únik informácií.

Zdroje:
https://portal.msrc.microsoft.com/en-us/security-guidance
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8292

Oracle Java

Spoločnosť Oracle tento mesiac vydala aktualizáciu opravujúcu 12 zraniteľností, z čoho 5 kritických. Väčšinu týchto zraniteľností je možné zneužiť vzdialene cez sieť, avšak je potrebná interakcia používateľa.

Zraniteľné systémy:
Java SE 11
Java SE 6u201, 7u191, 8u181
Java SE Embedded 8u181
JRockit R28.3.19

Odporúčania:
Vzhľadom závažnosť uvedených zraniteľností odporúčame čo najskôr aktualizovať zraniteľné verzie Java SE a Java SE Embedded na aktuálne verzie, t.j. Java SE 8u191, Java 11.0.1, 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/cpuoct2018-4428296.html

6. Iné závažné zraniteľnosti

Zraniteľnosť D-Link routerov

Bolo nájdených viac zraniteľností v istých modeloch D-Link routerov, ktoré umožňujú vykonať traverzovanie cesty, získať prístupové administrátorské heslá do routera. Pre viac informácii si prečítajte naše varovanie.

Zraniteľné systémy:

D-Link routre DWR-116, DIR-140L, DWR-512, DIR-640L, DWR-712, DWR-912, DWR-921, DWR-111

Zraniteľnosti CMS Drupal

Dve kritické zraniteľnosti boli objavené v podporovaných verziách CMS Drupal a umožňujú vzdialené vykonávanie kódu. Bližšie informácie sa dozviete v našom varovaní.

Zraniteľné systémy:

Drupal Core verzie 7.x a 8.x

Odporúčania:

Vzhľadom na veľké množstvo používateľov je Drupal pre útočníkom zaujímavým cieľom. Preto odporúčame bezodkladnú aktualizáciu na verzie:

- Drupal 7.60
- Drupal 8.6.2
- Drupal 8.5.8

Zero-day zraniteľnosť jQuery

V module frameworku jQuery s názvom jQuery File Upload bola odhalená osem rokov stará závažná zraniteľnosť. Kvôli nej je možné bez autentifikácie na server nahrať ľubovoľný kód a spúšťať vzdialené príkazy s privilégiami servera. Pre viac informácií si prečítajte naše varovanie.

Zraniteľné systémy:

jQuery File Upload 9.22.1 a staršie

Zraniteľnosti v produktoch Oracle

V balíku opráv vydanom tento mesiac spoločnosťou Oracle je opravených približne 300 zraniteľností. Najzávažnejšia z nich sa týka produktu GoldenGate a je možné ju zneužiť jednoduchým spôsobom vzdialene a bez autentifikácie. Bolo opravených taktiež 45 podobných zraniteľností. Viac informácií môžete nájsť v našom varovaní.

Zraniteľné systémy:

Najzraniteľnejšie produkty:

- Oracle GoldenGate, podporované verzie 12.1.2.1.0, 12.2.0.2.0 a 12.3.0.1.0
- Oracle Database Server
- Oracle Big Data Graph

- Oracle Communications Applications
- Oracle Contruction and Engineering Suite
- Oracle E-Business Suite
- Oracle Retail Applications
- Oracle Fusion Middleware
- Oracle Insurance Applications
- Oracle JD Edwards
- Oracle Enterprise Manager Products Suite
- MySQL
- Oracle Sun Systems Products Suite
- Oracle Siebel CRM

Odporúčania:

Bezodkladná aktualizácia programového vybavenia od spoločnosti Oracle.

Chyba v LibSSH

Zraniteľnosť v LibSSH umožňuje útočníkovi sa prihlásiť na server bez zadania hesla. Pre bližšie informácie si prečítajte naše varovanie.

Zraniteľné systémy:

LibSSH verzie staršej ako 0.8.4 a 0.7.6

Odporúčania:

Aktualizácia LibSSH na verziu 0.8.4 a 0.7.6